УДК 519.87

Е.В. Ивохин, Д.А. Ваднев

О НЕКОТОРЫХ СВОЙСТВАХ И ОЦЕНКАХ ДЛЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПРОСТЫХ ЧИСЕЛ

Введение

В истории науки есть по крайней мере одна глава, связывающая воедино труды величайших ученых со времен античности и до наших дней. Глава эта посвящена *простым числам* — атомам арифметики. Казалось бы, за безобидным названием этих чисел, которые делятся только на единицу и на самих себя, скрывается одна из сложнейших проблем, когда-либо возникавших перед исследователями-математиками [1].

Со времен Евклида математики пытаются разглядеть некоторую закономерность в распределении простых чисел на числовой оси. Если посмотреть даже на наименьшие простые числа, то вряд ли можно усмотреть какую-либо логику в их расположении на числовой оси. И такая логика становится все более и более эфемерной по мере того, как мы продолжаем углубляться в числовые дебри.

Развитие теории простых чисел в некотором смысле отражает эволюцию методов математического познания: от выдвижения эмпирических (интуитивных) гипотез и такой же эмпирической их проверки до предоставления доказательного обоснования, возводящего утверждения в ранг теорем. Принцип логически обоснованного доказательства утверждений, впервые открытый в древней Греции, позволяет перейти из области человеческой интуиции в пространство истинного, объективного знания, отражающего устройство природы.

Чтобы продвинуться в понимании простых чисел, потребовались многие годы и математическое чутье величайших математиков истории. Один из них — Карл Гаусс, который, изучая таблицы простых чисел в книге с логарифмами, сумел разглядеть закономерность в расположении этих необычных чисел на числовой оси. Гениальность его догадки заключается в том, чтобы не предсказывать, является ли произвольное натуральное число N простым, а *оценить,* сколько в среднем простых чисел находится на заданном отрезке. Слово «оценить» в данной постановке вопроса принципиально, поскольку знание *истинного* количества простых чисел на отрезке $[2, K]$, которое обозначают как $\pi(K)$, позволяет точно сказать, является ли произвольное целое число N простым. Именно точная зависимость $\pi(K)$, имеющая вид ступенчатой функции, всегда служила заветной целью для математиков. И оценочный подход Гаусса дал первое существенное приближение к этой зависимости.

Рассмотрим альтернативные способы оценивания и использования простых чисел.

1. Специальные последовательности простых чисел и их свойства

Последовательности простых чисел можно эффективно использовать при решении многих прикладных задач с применением вычислительных схем [2]. Введем отдельные понятия и операции.

Определение 1. Последовательности неотрицательных простых чисел $P_j(a) \ge 0,\ \ j \in Z,$ принадлежащих интервалу $[a, \infty)$ при $j \ge 0$ или интервалу $[0, a)$ при $j < 0$ для заданного, необязательно простого, целого числа $a \ge 0,$ будем называть последовательностями простых чисел относительно числа $a.$

Пусть заданы простые числа $P_j(a) \ge 0$ с порядковыми номерами $j \in Z$ из последовательности простых чисел относительно числа $a \ge 0.$ Нетрудно проверить, что справедливы соотношения, характеризующие свойства последовательности простых чисел:

1) $P_0(0) = 0,\ \ P_0(1) = 1,\ \ P_1(0) = 1;$

2) $P_0(a) = a,$ если число $a \ge 0$ простое, иначе $P_0(a)$ не существует;

3) $P_j(a) \le P_k(a),$ если $j \le k,\ \ P_j(a) < P_k(a)$ при $j < k,\ \ j \in Z,\ \ k \in Z;$

4) $P_j(a) = P_j(a+1) = ... = P_j(a+l)$ для всех $1 \le l < P_{j+1}(a) - P_j(a),\ \ j = 0, 1, 2, ...,$ $a \ge 0;$

5) $P_j(a) = P_1(P_{j-1}(a)) = P_1(P_1(P_{j-2}(a))) = P_2(P_{j-2}(a)) = ... = P_{j-1}(P_1(a)),$ если число $a \ge 0$ простое, $j \in Z;$

6) $P_j(a) \ge a$ для всех $j = 0, 1, 2, ...,$ если число $a \ge 0$ простое, $P_j(a) > a$ для всех $j = 1, 2, ...,$ если $a \ge 0$ непростое;

7) $P_j(a) < a$ для всех $j = -1, -2, ..., j_0,$ где номер $j_0 < 0$ определяется как наименьший индекс простого числа из последовательности, для которого $0 \le P_{j_0}(a) < a.$

Если $a > 0$ — простое число, то существует число $P_0(a).$ Используя указанные выше свойства, получаем соотношения $P_j(a) / P_k(a) \le 1,\ P_j(a) / P_k(a) = P_j(a) / P_1(P_{k-1}(a)) = ... = P_j(a) / P_j(P_{k-j}(a)) = P_j(a) / P_{k-j}(P_j(a))$ для любых $j, k \in Z,\ \ j \le k.$

Кроме традиционных арифметических операций сложения, вычитания, умножения и деления простых чисел, для последовательностей простых чисел $P_j(a),\ \ j = 0, 1, 2, ...,$ относительно произвольного $a \ge 0$ введем операцию смещения на $m,\ \ m \in Z,\ \ j + m \ge j_0,$ простых чисел в виде

$$P_j(a) \oplus m = P_{j+m}(a) = P_m(P_j(a)), \tag{1}$$

которая по определению не выводит за нижнюю границу заданной последовательности $(j + m \ge j_0),$ и операцию n-кратной композиции $(n \in Z)$ отношения двух чисел: $P_j(a)$ и $P_k(a),\ \ j, k \in Z,\ \ j \le k,$ в виде

$$P_j(a) / P_k(a) \circ n = P_j(a) \oplus n / P_k(a) \oplus n = P_{j+n}(a) / P_{k+n}(a) = P_n(P_j(a)) / P_n(P_k(a)). \tag{2}$$

Предположим, что рассматривается произвольное рациональное число r. Без ограничения общности, будем считать, что число r неотрицательное, $r \ge 0.$

Лемма 1. Произвольное рациональное число $r = p / q,\ \ p \in Z,\ \ q \in N,$ может быть представлено в виде

$$r = \prod_{i=1}^{s_p} P_{k_i}(a_{k_i}) \Big/ \prod_{j=1}^{s_q} P_{n_j}(a_{n_j}), \tag{3}$$

где s_p, s_q — число сомножителей в представлении p и q в виде соответствующих произведений элементарных делителей, $a_{k_i} \ge 0,\ \ a_{n_j} \ge 0$ — некоторые целые числа, $k_i, n_j \in Z,\ \ i = \overline{1, s_p},\ \ j = \overline{1, s_q}.$

Доказательство. Известно, что произвольное рациональное число r представляется в виде простой дроби $r = p/q,\ \ p \in Z,\ \ q \in N.$ Если при этом оба числа (p и q) являются простыми числами, то получаем утверждение леммы. В данном случае $s_p = 1, s_q = 1,\ \ P_{k_1}(a_{k_1}) = p,\ \ P_{n_1}(a_{n_1}) = q$ для некоторых $k_1 \in Z,$ $n_1 \in Z$ и $a_{k_1} \geq 0,\ a_{n_1} \geq 0.$

Если числитель или знаменатель или оба числа (p и q) не являются простыми, то их можно представить в виде произведения элементарных делителей, являющихся простыми числами. Количество записей элементарных делителей в произведениях соответствует их кратности. Обозначим количество сомножителей в представлении чисел p и q в виде соответствующих произведений через $s_p, s_q,$ где каждый из сомножителей является простым числом из некоторых последовательностей простых чисел относительно чисел $a_{k_i},\ \ a_{n_j},\ \ k_i, n_j \in Z,$ $i = \overline{1, s_p},\ \ j = \overline{1, s_q}.$

Представление (3) для произвольного рационального числа r доказано.

Следствие 1. Произвольное рациональное число $r = p/q,\ \ p \in Z,\ \ q \in N,$ может быть представлено в виде

$$r = \prod_{i=1}^{s_p} P_{k_i}(a) \Big/ \prod_{j=1}^{s_q} P_{n_j}(a), \tag{4}$$

где s_p, s_q — число сомножителей в представлении p и q в виде соответствующих произведений элементарных делителей, $a \geq 0$ — некоторое целое число, $k_i \in Z,$ $n_j \in Z,\ \ i = \overline{1, s_p},\ \ j = \overline{1, s_q}.$

Следствие 2. Произвольное рациональное число $r = p/q,\ \ p \in Z,\ \ q \in N,$ может быть представлено в виде

$$r = \prod_{i=1}^{s} P_{k_i}(0) \Big/ \prod_{j=1}^{s} P_{n_j}(0), \tag{4'}$$

где s — максимальное значение сомножителей в представлении чисел p и q в виде соответствующих произведений элементарных делителей, $k_i, n_j \in N \cup \{0\},$ $i = \overline{1, s_p},\ \ j = \overline{1, s_q}.$

Лемма 2. Для произвольного рационального числа r и заданного $n \in N$ существуют целые числа $a \geq 0,\ \ b \geq 0$ и простые числа с номерами $i^* \in Z$ и $j^* \in Z$ из последовательностей простых чисел относительно a и b соответственно, такие, что для всех $i, j \in N,\ \ i \leq n,\ \ j \leq n,$ справедливо неравенство

$$\left| P_{i^*}(a) \Big/ P_{j^*}(b) - r \right| \leq \left| P_i(a) \Big/ P_j(b) - r \right|. \tag{5}$$

Доказательство. Рассмотрим возрастающую последовательность всех простых чисел $p_i \geq 0,\ \ i \in N,$ причем 0 и 1 также считаем простыми числами. Предположим, что задано рациональное число r и целое $n \in N.$

Покажем существование простых чисел с номерами $i^o \in N,\ \ j^o \in N,$ для которых выполняется соотношение $\left| p_{i^o} / p_{j^o} - r \right| \le \left| p_i / p_j - r \right|$ для всех $i, j \in N,$ $i \le n,\ \ j \le n,$ на основе следующего алгоритма.

0. Положим $i = 0,\ \ j = 1.$

1. Пока $i \le n$ и $j \le n,$ повторяем пп. 2– 4.

2. Если $p_i / p_j = r,$ то решение найдено, $i^o = i,\ \ j^o = j.$ Переходим к п. 5.

3. Если $p_i / p_j < r,$ то увеличиваем номер $i = i + 1$ и вычисляем новое простое число $p_i \ge 0;$ в противном случае увеличиваем номер $j = j + 1$ и находим простое число $p_j \ge 0.$

4. Если $\left| p_i / p_j - r \right| < \left| p_{i^o} / p_{j^o} - r \right|,$ то фиксируем $i^o = i,\ \ j^o = j.$

5. Значения $i^o,\ \ j^o$ — решение поставленной задачи.

Очевидно, что соответствующие простые числа p_{i^o}, p_{j^o} могут рассматриваться в качестве элементов последовательностей простых чисел относительно некоторых $a \ge 0,\ b \ge 0$ с номерами $i^* \in Z$ и $j^* \in Z$ соответственно.

Далее покажем, что значения $i^*,\ \ j^*,$ найденные с помощью описанного выше алгоритма, являются оптимальным решением задачи.

Пусть, от противного, существуют значения $i_0, j_0 \in N,\ \ i_0 \le n,\ \ j_0 \le n,$ такие, что для соответствующих элементов из последовательности простых чисел справедливо $\left| p_{i_0} / p_{j_0} - r \right| < \left| p_{i^o} / p_{j^o} - r \right|.$ Так как значения номеров i и j в алгоритме монотонно увеличиваются, то существует значение $i' \in N,\ \ i' \le n,$ такое, что на некоторой итерации алгоритма имеем $i = i',\ \ j = j_0.$ Аналогично существует значение $j' \in N,\ \ j' \le n,$ такое, что на некоторой итерации алгоритма $i = i_0,\ \ j = j'.$ При этом либо $i' \le i_0,$ либо $j' \le j_0$ (иначе алгоритм проходил бы через значения $i = i',\ \ j = j_0$ и $i = i_0,\ \ j = j',$ для которых $i' > i_0$ и $j' > j_0$).

Без ограничения общности рассмотрим случай $i' \le i_0.$ Пусть $i^{\min} \in N,$ $i^{\min} \le i^o$ — наименьшее значение номера i такое, что $p_{i^{\min}} / p_{j_0} \ge r.$

Если $i^{\min} \ge i_0,$ то на определенном шаге алгоритм проходит через значения номеров $i = i_0, j = j_0.$ Тогда имеем $\left| p_{i_0} / p_{j_0} - r \right| \ge \left| p_{i^o} / p_{j^o} - r \right|,$ что противоречит предположению. Таким образом, $i^{\min} < i_0,$ и, как следствие, $p_{i^{\min}} / p_{j_0} << p_{i_0} / p_{j_0}.$ $p_{i^{\min}} / p_{j_0} < p_{i_0} / p_{j_0}.$

Из данных соотношений имеем $\left| p_{i^o} / p_{j^o} - r \right| \le \left| p_{i^{\min}} / p_{j_0} - r \right| < \left| p_{i_0} / p_{j_0} - r \right|,$ что снова противоречит предположению.

Окончательно можно сделать вывод, что не существует номеров $i_0, j_0 \in N,$ $i_0 \le n,\ \ j_0 \le n,$ таких, что $\left| p_{i_0} / p_{j_0} - r \right| < \left| p_{i^o} / p_{j^o} - r \right|.$

Лемма доказана.

Следствие 1. Для произвольного рационального числа r и заданного $n \in N$ существуют простые числа с номерами $i^* \in N$ и $j^* \in N$ из последовательности простых чисел относительно числа $a = 0$ такие, что для всех $i, j \in N$, $i \le n$, $j \le n$, справедливо неравенство

$$\left| P_{i^*}(0) \big/ P_{j^*}(0) - r \right| \le \left| P_i(0) \big/ P_j(0) - r \right|. \qquad (5')$$

Доказательство. Нетрудно заметить, что если положить $a = b = 0$, то, повторяя доказательство леммы, получаем справедливость соотношения (5′).

Лемма 3. Для произвольных двух простых чисел: $P_k(a)$, $P_n(a)$, $k \le n$, $k, n \in Z$, из последовательности простых чисел относительно числа a и произвольного числа $T \ge 0$ справедливо соотношение

$$(P_k(a) + T) \big/ (P_n(a) + T) \ge P_k(a) \big/ P_n(a). \qquad (6)$$

Доказательство. Несложно проверить, что для любых $k \le n$, $k, n \in Z$, имеет место

$$(P_k(a) + T) \big/ (P_n(a) + T) - P_k(a) \big/ P_n(a) = T(P_n(a) - P_k(a)) \big/ ((P_n(a) + T) * P_n(a)).$$

Учитывая свойство 3) последовательностей простых чисел, получаем, что

$$(P_k(a) + T) \big/ (P_n(a) + T) - P_k(a) \big/ P_n(a) \ge 0,$$

откуда следует неравенство (6).

Лемма доказана.

Рассмотрим множество неотрицательных рациональных чисел $r(k, n)$, $k, n \in Z$, $0 \le r(k, n) \le 1$, которые представляются в виде отношения двух простых чисел из последовательности относительно числа $a \ge 0$:

$$r(k, n) = P_k(a) \big/ P_n(a), \quad k \le n, \quad k, n \in Z. \qquad (7)$$

Без ограничения общности положим $a = 0$. При этом рациональные числа $r(k, n)$ будут представляться в виде

$$r(k, n) = P_k(0) \big/ P_n(0), \quad k \le n, \quad k, n \in N \cup \{0\}. \qquad (8)$$

С учетом операции смещения на m простых чисел в последовательности $P_j(0)$, $j \in Z$ получаем соотношения

$$r(k + m, n + m) = r(k, n) \circ m, \quad m \in N \cup \{0\}. \qquad (9)$$

Введем в рассмотрение другие числовые совокупности.

Определение 2. Множество рациональных чисел $r_T(k, n)$, $T \ge 0$, $k \le n$, $k, n \in N \cup \{0\}$, вида

$$r_T(k, n) = (P_k(0) + T) \big/ (P_n(0) + T), \quad k \le n, \quad k, n \in N \cup \{0\}, \qquad (10)$$

назовем *T*-последовательностью для множества чисел $r(k, n)$ и заданного $T \ge 0$.

Определение 3. Для заданного множества чисел $r(k, n)$, $k \le n$, $k, n \in N \cup \{0\}$, множество чисел

$$r_*(k + m, n + m) = \frac{P_k(0) \oplus m_*}{P_n(0) \oplus m}, \; k \le n, \quad m \in Z, \quad k, n \in N \cup \{0\}, \qquad (11)$$

где m_*: $0 \le m_* \le m$ при $m \in N \cup \{0\}$, и $m_* \le m$ при $m < 0$, — наибольшее целое число такое, что

$$P_k(0) \oplus m / P_n(0) \oplus m \ge P_k(0) \oplus m_* / P_n(0) \oplus m,$$

будем называть нижним сопряженным множеством, а множество чисел

$$r^*(k+m, n+m) = \frac{P_k(0) \oplus m^*}{P_n(0) \oplus m}, \quad k \le n, \quad m \in Z, \quad k, n \in N \cup \{0\}, \tag{12}$$

где m^*: $m^* \ge m$ при $m \in N \cup \{0\}$ и $m \le m^* \le 0$ при $m < 0$, — наименьшее целое число такое, что

$$P_k(0) \oplus m / P_n(0) \oplus m \le P_k(0) \oplus m^* / P_n(0) \oplus m,$$

— верхним сопряженным множеством.

Лемма 4. Справедливы следующие соотношения:

$$r(k, n) \le r_T(k, n), \tag{13}$$

$$r_*(k+m, n+m) \le r(k+m, n+m), \tag{14}$$

$$r(k+m, n+m) \le r^*(k+m, n+m), \tag{15}$$

$$r_*(k+m, n+m) \le r_T(k+m, n+m) \tag{16}$$

для произвольных $T \ge 0$, $k, n \in N \cup \{0\}$, $k \le n$, $m \in Z$.

Доказательство. В соответствии с леммой 3 для произвольного числа $T \ge 0$ справедливо неравенство $r_T(k, n) = (P_k(0) + T)/(P_n(0) + T) \ge P_k(0)/P_n(0) = r(k, n)$ и выполняются соотношения

$$r(k+m, n+m) = \frac{P_k(0) \oplus m}{P_n(0) \oplus m} \ge \frac{P_k(0) \oplus m_*}{P_n(0) \oplus m} = r_*(k+m, n+m),$$

$$r(k+m, n+m) = \frac{P_k(0) \oplus m}{P_n(0) \oplus m} \le \frac{P_k(0) \oplus m}{P_n(0) \oplus m^*} = r^*(k+m, n+m)$$

для произвольных значений $k, n \in N \cup \{0\}$, $k \le n$ и любого $m \in Z$. Таким образом, неравенства (13)–(15) доказаны.

Неравенство (13) выполняется для всех $k, n \in N \cup \{0\}$, $k \le n$. Тогда для любого $m \in Z$ имеем $k + m \le n + m$, откуда для любого $T \ge 0$ справедливо соотношение $r(k+m, n+m) \le r_T(k+m, n+m)$. С учетом неравенства (14) окончательно получаем $r_*(k+m, n+m) \le r_T(k+m, n+m)$, что соответствует неравенству (16).

Следствие 1. Для произвольных значений $T \ge 0$, $k \in N \cup \{0\}$, $n \in N \cup \{0\}$, $k \le n$ справедливы соотношения

$$r_*(k, n) \le r(k, n), \tag{17}$$

$$r(k, n) \le r^*(k, n), \tag{18}$$

$$r_*(k, n) \le r_T(k, n). \tag{19}$$

Доказательство. Справедливость неравенств (17)–(19) очевидна. Действительно, положим $m = 0$ в соотношениях (14)–(16). В результате получаем неравенства (17)–(19) для произвольных значений $T \geq 0$, $k \in N \cup \{0\}$, $n \in N \cup \{0\}$, $k \leq n$, что и требовалось доказать.

Очевидно, что свойство элементов совокупности $r(k, n)$ в виде $0 \leq r(k, n) \leq 1$ сохраняется для всех членов T-последовательности с произвольным значением $T \geq 0$ и элементов нижнего и верхнего сопряженных множеств:

$$0 \leq r_T(k, n) \leq 1, \quad 0 \leq r_*(k+m, n+m) \leq 1, \quad 0 \leq r^*(k+m, n+m) \leq 1 \tag{20}$$

для всех $k \in N \cup \{0\}$, $n \in N \cup \{0\}$, $k \leq n$, и любого $m \in N \cup \{0\}$.

Из леммы 4 и следствия можно сделать вывод, что существуют соотношения между соответствующими элементами множеств $r(k, n)$, $k \in N \cup \{0\}$, $n \in N \cup \{0\}$, $k \leq n$, и элементами T-последовательности с произвольным значением $T \geq 0$ нижнего и верхнего сопряженных множеств. При этом, к сожалению, ничего нельзя сказать о соотношении чисел $r(k, n)$ и $r(k+m, n+m)$ для произвольного $m \in N \cup \{0\}$.

2. Числовые последовательности, построенные на простых числах

Рассмотрим две неубывающие числовые последовательности:

$$g(n) = \max\{g(n-1), r(n)\}, \quad n \in N, \quad g(0) = 0, \tag{21}$$

где $r(n)$, $n \in N$, — расстояние между двумя ближайшими к числу $n \in N$ простыми числами $q_s(n), q_{s+1}(n)$, $s \in N$, такими, что $n \geq q_s(n)$, $n < q_{s+1}(n)$, т.е. $r(n) = q_{s+1}(n) - q_s(n)$;

$$p(n) = \max\{p(n-1), l(n)\}, \quad n \in N, \quad p(0) = 0, \tag{22}$$

где $l(n) = P_1(n) - P_{-1}(n)$, $n \in N$, $P_{-1}(n), P_1(n)$ — предыдущее и следующее простые числа относительно числа $n \in N$.

Очевидно, что если $n \in N$ — простое число с номером $s \in N$ из последовательности простых чисел, то $q_s(n) = n$ и $r(n) = q_{s+1}(n) - n$, $n \in N$. Значения $r(n)$ в этом случае совпадают с элементами числовой последовательности $d(s) = q_{s+1} - q_s$, $s \in N$, q_s, q_{s+1} — два последовательных простых числа, $s \in N$. Данная последовательность, состоящая из величин расстояний между парами последовательных простых чисел, часто используется в исследованиях совокупностей простых чисел [3]. В некоторых случаях рассматривается числовая последовательность $f(n) = \max\{f(n-1), q(n)\}$, $f(0) = 0$, где $q(n)$, $n \in N$, — расстояние от числа n до ближайшего к нему простого числа, т.е. $q(n) = q_s - n$ для некоторого $s \in N$ [4].

Очевидно, что если $n \in N$ — простое число, существует $s \in N$ такое, что

$$l(n) = P_1(n) - P_{-1}(n) = (P_1(n) - n) + (n - P_{-1}(n)) = r(n) + r(n-1)) =$$

$$= r(n+1) + r(n-1)) = r(n) + r(n-2))... = r(n + d(s) - 1) - r(n - d(s-1)),$$

или, в более общей форме, $l(n) = r(n+i-1) + r(n-j)$ для всех $i = \overline{1, d(s)}$, $j = \overline{1, d(s-1)}$ и некоторого числа $s \in N$.

Таким образом, окончательно получаем:

1) последовательности $g(n)$, $p(n)$ неубывающие, кусочно-постоянные с интервалами постоянства $[q_s(n), q_{s+1}(n))$, $s \in N$;

2) для всех $n \in N$ справедливо $l(n) \geq r(n)$ и, следовательно, $p(n) \geq g(n)$.

При построении оценок для простых чисел рассматривается последовательность $B(n)$, $n \in N$, $B(0) = 1$, элементами которой являются целые числа, определяющие количество разрядов в двоичном представлении числа $n \in N$. Отметим, что для чисел $n = 2^k$, $k = 1, 2, \ldots$, справедливы соотношения $B(n)B(n-1)+1 = B(n-2)+1 = \ldots = B(n-m)+1$, $m = 1, 2, \ldots, 2^{k-1}$, $k = 1, 2, \ldots$, и $B(1) = B(0)$.

Свойства. Для элементов рассматриваемых последовательностей выполняются следующие соотношения [5]:

1) для всех $n \geq 5$ справедливо неравенство $B(n)+1 \leq p(n)$;

2) для всех $n \in N$ справедливо неравенство $g(n) < 2,3B(n)$;

3) для всех $n \geq 7$ справедливо неравенство $B(n) \leq 5/6\, p(n)$.

Лемма 5. Для всех значений $n \in N$, $n \geq 7$, таких, что число $2n+1$ не является простым, справедливо неравенство

$$2p(n) > p(2n). \tag{23}$$

Доказательство. Используем метод математической индукции:

1) $n = 7$; $p(7) = 6$; $p(14) = 6$, $2p(7) > p(14)$;

2) пусть неравенство (23) справедливо для всех $n = \overline{7, m}$ при условии, что $2n+1$ составное. При $n = m$ имеем $2p(m) > p(2m)$ и число $2m+1$ не является простым.

Покажем, что лемма справедлива и для $n = m+1$, т.е. $2p(m+1) > p(2m+2)$.

Из определения последовательности $p(n)$, $n \in N$, запишем

$$p(2m+2) = \max\{p(2m+1), l(2m+2)\}, \quad p(2m+1) = \max\{p(2m), l(2m+1)\}.$$

Если выполняется соотношение $p(2m) = p(2m+1) = p(2m+2)$, то, учитывая, что данная последовательность неубывающая, получаем $2p(m+1) \geq 2p(m) > p(2m) = p(2m+2)$.

В более сложном случае предположим, что $p(2m) < p(2m+2)$. Так как числа $2m$, $2m+2$ четные и, следовательно, не являются простыми, а число $2m+1$ составное по условию, то получаем $P_{-1}(2m) = P_{-1}(2m+1) = P_{-1}(2m+2)$, $P_1(2m) = P_1(2m+1) = P_1(2m+2)$ и $l(2m) = l(2m+1) = l(2m+2)$. Отсюда $p(2m) = p(2m+1) = p(2m+2)$, что противоречит предположению. Таким образом, окончательно получаем неравенство

$$2p(m+1) \geq 2p(m) > p(2m) = p(2m+2) = p(2(m+1)).$$

Следствие 1. Для всех значений $n \in N$, $n \geq 7$, таких, что число $2n+1$ не является простым, справедливы неравенства

$$2p(n) > p(2n+1), \tag{23′}$$

$$2p(n) > p(2n+2). \tag{23″}$$

Доказательство. При условии, что число $2n+1$ является составным, справедливы равенства $p(2n) = p(2n+1) = p(2n+2)$. Учитывая неравенство (23), получаем соотношения (23′), (23″).

Замечание. Необходимо отметить, что при замене в соотношениях (23), (23′), (23″) строгих неравенств на нестрогие можно получить аналогичные соотношения для всех $n \in N$. В качестве примеров приведем неравенства для $n < 7$:

$n = 1;\ \ p(1) = 2;\ \ p(2) = 2,\ \ p(3) = 3;\ \ 2p(1) > p(2),\ \ 2p(1) > p(3),\ \ 2p(1) > p(4);$

$n = 2;\ \ p(2) = 2,\ \ p(4) = 3,\ \ p(5) = 4;\ \ 2p(2) > p(4),\ \ 2p(2) = p(5),\ \ 2p(2) = p(4);$

$n = 3;\ \ p(3) = 3;\ \ p(6) = 4,\ \ p(7) = 6;\ \ 2p(3) > p(6),\ \ 2p(3) = p(7),\ \ 2p(3) = p(8);$

$n = 4;\ \ p(4) = 3;\ \ p(8) = 6,\ \ p(9) = 6;\ \ 2p(4) = p(8),\ \ 2p(4) = p(9),\ \ 2p(4) = p(10);$

$n = 5;\ \ p(5) = 4;\ \ p(10) = 6,\ \ p(11) = 6;\ \ 2p(5) > p(10),\ \ 2p(5) > p(11),\ \ 2p(5) > p(12);$

$n = 6;\ \ p(6) = 4;\ \ p(12) = 6,\ \ p(13) = 6;\ \ 2p(6) > p(12),\ \ 2p(6) > p(13),\ \ 2p(6) > p(14) = 6.$

Следствие 2. Для всех значений $n \in N,\ \ n \geq 5,$ таких, что число $2n-1$ не является простым, справедливы неравенства

$$2p(n) > p(2n). \tag{24}$$

$$2p(n) > p(2n-1), \tag{24′}$$

$$2p(n) > p(2n-2). \tag{24″}$$

Доказательство. Проверим справедливость утверждения для $n = 5$. Учитывая, что $p(5) = 4,\ \ p(10) = 6,\ \ p(9) = 6,\ \ p(8) = 6,$ непосредственной подстановкой в соотношения (24), (24′), (24″) убеждаемся в их истинности. Предположим далее, что справедлива лемма 5, т.е. для всех $m \in N,\ \ m \geq 7,$ таких, что число $2m+1$ является составным, справедливы неравенства $2p(m) > p(2m),\ \ 2p(m) > p(2m+1),\ \ 2p(m) > p(2m+2)$. Положив $m = n-1,$ перепишем полученные соотношения относительно $n \in N,\ \ n \geq 8$. Имеем: число $2m+1 = 2n-2+1 = 2n-1$ — составное и справедливы неравенства $2p(n-1) > p(2n-2),\ \ 2p(n-1) > p(2n-1),\ \ 2p(n-1) > p(2n)$. Учитывая, что последовательность $p(n)$ неубывающая, т.е. $p(n-1) \leq p(n)$ для всех $n \in N,$ получаем соотношения (24), (24′), (24″). Для $n = 6$ и $n = 7$ числа $2n-1$ простые и не удовлетворяют условию следствия. Таким образом, окончательно получаем, что при выполнении условий для $n \in N,\ \ n \geq 5,$ таких, что число $2n-1$ не является простым, справедливы неравенства (24), (24′), (24″).

Лемма 6. Для всех значений $n \in N,\ \ n \geq 4,$ таких, что число $2n+3$ простое, справедливо неравенство

$$P_1(2n+3) < 2n+3+2p(n). \tag{25}$$

Доказательство. Применим метод математической индукции. Учитывая очевидное неравенство при $n = 4,\ \ p(4) = 3$ и условии, $2n+3 = 11$ — простое число имеем

$$P_1(11) = 13 < 17 = 8+3+6 = 2*4+3+2p(4),$$

и предполагая справедливость соотношения (25) для всех $n \in N,\ \ n = \overline{4, m},$ проверим истинность утверждения для $n = m+1$.

По условиям леммы число $2m+3$ простое, а число $2n+3=2m+5$ может быть простым или составным. Имеем:

1) $2m+5$ не является простым. В этом случае получаем $P_1(2m+5)=$ $=P_1(2m+3)<2m+3+2p(m)<2m+5+2p(m)\le 2m+5+2p(m+1)$, отсюда $P_1(2m+5)=$ $=P_1(2(m+1)+3)<2m+5+2p(m+1)=2(m+1)+3+2p(m+1)$, что и требовалось получить;

2) $2m+5$ является простым. Положим $k=m+1$. Из (25) имеем $P_1(2m+5)=$ $=P_1(2k+3)<2k+3+p(k)=2(m+1)+3+p(m+1)$ и, следовательно, справедливо утверждение леммы для $n=m+1$.

Лемма доказана.

Лемма 7. Для всех значений $n\in N$, $n\ge 4$, таких, что число $2n+3$ является простым, справедливо неравенство

$$P_{-1}(2n+3)>2n+3-2p(n). \tag{26}$$

Доказательство. Применяя метод математической индукции, при $n=4$, $p(4)=3$ и условии, что $2n+3=11$ — простое число, имеем очевидное неравенство

$$P_{-1}(11)=7>5=8+3-6=2*4+3-2p(4).$$

Предположим справедливость соотношения (26) для всех $n\in N$, $n=\overline{4,m}$. Проверим истинность утверждения для $n=m+1$.

По условиям леммы число $2m+3$ простое, а числа $2n+3=2m+5$, $2m+3-2p(m)$, $2m+5-2p(m)$ нечетные. Получаем $P_{-1}(2m+5)=2m+3>$ $>P_{-1}(2m+3)>2m+3-2p(m)$ и $P_{-1}(2m+3)\ge 2m+5-2p(m)$.

Учитывая, что $p(m)\le p(m+1)$, окончательно имеем $P_1(2m+5)>$ $>2(m+1)+3-2p(m+1)$, что и требовалось получить.

Следовательно, утверждение леммы остается истинным для $n=m+1$.

Лемма доказана.

Утверждение 1. Пусть для произвольного значения $n\in N$ величина $p(n)=\overline{p}$. Тогда справедливы неравенства

$$2n-2\overline{p}+1\le P_{-1}(2n), \tag{27}$$

$$2n-2\overline{p}+3\le P_{-1}(2n+1). \tag{28}$$

Доказательство. Воспользуемся методом математической индукции.

1. $n=1;\ \ p(1)=2;\ \ 2-4+1\le P_{-1}(2)=1,\ \ 2-4+3\le P_{-1}(3)=2;$

$n=2;\ \ p(2)=2;\ \ 4-4+1\le P_{-1}(4)=3,\ \ 4-4+3\le P_{-1}(5)=3;$

$n=3;\ \ p(3)=3;\ \ 6-6+1\le P_{-1}(6)=5,\ \ 6-6+3\le P_{-1}(7)=5;$

$n=4;\ \ p(4)=3;\ \ 8-6+1\le P_{-1}(8)=7,\ \ 8-6+3\le P_{-1}(9)=7;$

$n=5;\ \ p(5)=4;\ \ 10-8+1\le P_{-1}(10)=7,\ \ 10-8+3\le P_{-1}(11)=7,$

$n=6;\ \ p(6)=4;\ \ 12-8+1\le P_{-1}(12)=11,\ \ 12-8+3\le P_{-1}(13)=11;$

$n=7;\ \ p(7)=6;\ \ 14-12+1\le P_{-1}(14)=13,\ \ 14-12+3\le P_{-1}(15)=13.$

2. Предположим, что утверждение справедливо для всех $n = \overline{1, m}$. При $n = m$ имеем

$$2m - 2\overline{p} + 1 \le P_{-1}(2m); \tag{27′}$$

$$2m - 2\overline{p} + 3 \le P_{-1}(2m+1). \tag{28′}$$

Покажем, что данное утверждение справедливо и для $n = m+1$. Для этого рассмотрим различные случаи.

- $p(m+1) = p(m) = \overline{p}$. Оценим величину $P_{-1}(2(m+1)) = P_{-1}(2m+2)$. Имеем $2(m+1) - 2\overline{p} + 1 = 2m - 2\overline{p} + 3$. С учетом предположения (28′) отсюда следует, что ближайшее простое число, не превосходящее $2m+2$, либо принадлежит интервалу $[2m - 2\overline{p} + 3, P_{-1}(2m+1))$, либо $P_{-1}(2m+2) = 2m+1$. Окончательно имеем $2m - 2\overline{p} + 3 = 2(m+1) - 2\overline{p} + 1 \le P_{-1}(2(m+1))$, что подтверждает справедливость неравенства (27).
- $p(m+1) = \widetilde{p} > \overline{p}$. В этом случае аналогично, используя соотношение $P_{-1}(2m+1) \ge 2m - 2\overline{p} + 3 > 2m - 2\widetilde{p} + 3$, получаем оценку для $P_{-1}(2m+2)$:

$$P_{-1}(2m+2) \in [2m - 2\overline{p} + 3, P_{-1}(2m+1)) \subseteq [2m - 2\widetilde{p} + 3, P_{-1}(2m+1))$$

или $P_{-1}(2m+2) = 2m+1$, откуда $2m - 2\overline{p} + 3 = 2(m+1) - 2\overline{p} + 1 \le P_{-1}(2(m+1))$.

Справедливость неравенства (27) доказана.

Рассмотрим далее соотношение (28). Предполагая справедливость (27′), (28′), оценим величину $P_{-1}(2(m+1)+1) = P_{-1}(2m+3)$.

Аналогично предыдущему проанализируем различные случаи.

- $p(m+1) = p(m) = \overline{p}$. Имеем $2(m+1) - 2\overline{p} + 3 = 2m - 2\overline{p} + 5$. Из (27′) следует гарантированная оценка для ближайшего простого числа, не превышающего $2m+3$: $P_{-1}(2m+3) \ge 2m - 2\overline{p} + 3$. Исходя из очевидного соотношения $2m - 2\overline{p} + 3 < 2m - 2\overline{p} + 5$, покажем, что число $2m - 2\overline{p} + 3$ не может быть ближайшим простым.

Действительно, предположим, что интервал $(2m - 2\overline{p} + 3, 2m + 3)$ не содержит простых чисел. Тогда ближайшими простыми числами в этом случае могут быть $2m - 2\overline{p} + 3$ и $2m + 3$. Отсюда следует, что расстояние между ними равняется $2\overline{p}$.

Из неравенства (26) леммы 7 имеем $P_{-1}(2m+3) > P_{-1}(2m+3) > 2m + 3 - 2p(m) = 2m + 3 - 2\overline{p}$.

Следовательно, предположение об отсутствии простых чисел на интервале $(2m - 2\overline{p} + 3, 2m + 3)$ неверно, откуда получаем $P_{-1}(2m+3) \ge 2m - 2\overline{p} + 5$.

- $p(m+1) = \widetilde{p} > \overline{p}$. Гарантированная оценка для ближайшего простого числа, не превышающего $2m+3$, будет иметь вид $P_{-1}(2m+3) \ge 2m - P_{-1}(2m+3) \ge 2m - 2\overline{p} + 3 > 2m - 2\widetilde{p} + 3$. Проведя аналогичные рассуждения, получаем, что число $2m - 2\overline{p} + 3$ не может быть ближайшим простым числом, не превышающим $2m+3$. Следовательно, $P_{-1}(2m+3) \ge 2m - 2\overline{p} + 5 > 2m - 2\widetilde{p} + 5$, что свидетельствует о справедливости неравенства (28).

Утверждение доказано.

Утверждение 2. Пусть для произвольного значения $n \in N$ величина $p(n) = \overline{p}$. Тогда справедливы неравенства

$$P_1(2n) \le 2n + 2\overline{p} - 3, \tag{29}$$

$$P_1(2n+1) \le 2n + 2\overline{p} - 1. \tag{30}$$

Доказательство. Вновь воспользуемся методом математической индукции.

1. $n = 1;\ p(1) = 2;\ P_1(2) = 3 \le 2 + 4 - 3,\ P_1(3) = 5 \le 2 + 4 - 1;$

$n = 2;\ p(2) = 2;\ P_1(4) = 5 \le 4 + 4 - 3,\ P_1(5) = 7 \le 4 + 4 - 1;$

$n = 3;\ p(3) = 3;\ P_1(6) = 7 \le 6 + 6 - 3,\ P_1(7) = 11 \le 6 + 6 - 1;$

$n = 4;\ p(4) = 3;\ P_1(8) = 11 \le 8 + 6 - 3,\ P_1(9) = 11 \le 8 + 6 - 1;$

$n = 5;\ p(5) = 4;\ P_1(10) = 11 \le 10 + 8 - 3,\ P_1(11) = 13 \le 10 + 8 - 1;$

$n = 6;\ p(6) = 4;\ P_1(12) = 13 \le 12 + 8 - 3,\ P_1(13) = 17 \le 12 + 8 - 1;$

$n = 7;\ p(7) = 6;\ P_1(14) = 17 \le 14 + 12 - 3,\ P_1(15) = 17 \le 14 + 12 - 1.$

2. Предположим, что утверждение справедливо для всех $n = \overline{1, m}$. При $n = m$ имеем

$$P_1(2m) \le 2m + 2\overline{p} - 3, \tag{29′}$$

$$P_1(2m+1) \le 2m + 2\overline{p} - 1. \tag{30′}$$

Покажем, что данное утверждение справедливо и для $n = m + 1$. Оценим величину $P_1(2(m+1)) = P_1(2m+2)$. Для этого рассмотрим различные случаи.

- $p(m+1) = p(m) = \overline{p}$. В этом случае $2(m+1) + 2\overline{p} - 3 = 2m + 2\overline{p} - 1$ и с учетом предположения (30′) следует, что ближайшее простое число, превосходящее $2m + 2$, принадлежит интервалу $[P_1(2m+3), 2m + 2\overline{p} - 1]$. Таким образом, $P_1(2(m+1)) \le 2m + 2\overline{p} - 1 = 2(m+1) + 2\overline{p} - 3$, что подтверждает справедливость неравенства (29).
- $p(m+1) = \overline{p} > \overline{p}$. Используя соотношение $P_1(2m+1) \le 2m + 2\overline{p} - 1 < 2m + 2\overline{p} - 1$, в этом случае получаем аналогичную оценку для $P_1(2m+2)$: $P_1(2m+2) \in (P_1(2m+1), 2m + 2\overline{p} - 1] \subseteq (P_1(2m+1), 2m + 2\overline{p} - 1]$ или $P_1(2(m+1)) \le P_1(2(m+1)) \le 2m + 2\overline{p} - 1 = 2(m+1) + 2\overline{p} - 3$.

Справедливость неравенства (29) доказана.

Рассмотрим далее соотношение (30). Предполагая справедливость (29′), (30′), оценим величину $P_1(2(m+1)+1) = P_1(2m+3)$. Аналогично предыдущему проанализируем различные случаи.

- $p(m+1) = p(m) = \overline{p}$. Имеем $2(m+1) + 2\overline{p} - 1 = 2m + 2\overline{p} + 1$. Из (30′) следует гарантированная оценка для ближайшего простого числа, превышающего $2m + 3$: $2m + 2\overline{p} - 1$. Если число $P_1(2m+3) \le 2m + 3$ не является простым, то $P_1(2m+1) = P_1(2m+2) = P_1(2m+3) \le 2m + 2\overline{p} - 1 < 2m + 2\overline{p} + 1$ и неравенство (30) доказано.

Пусть $2m + 3$ — простое число. Исходя из очевидного соотношения $2m + 2\overline{p} - 1 < 2m + 2\overline{p} + 1 < 2m + 2\overline{p} + 3$, покажем, что число $2m + 2\overline{p} + 3$ не может быть ближайшим к $2m + 3$ простым числом.

Действительно, предположим от противного, что интервал $(2m+3,\ 2m+2\overline{p}+3)$ не содержит простых чисел. Тогда ближайшими простыми числами в этом случае могут быть $2m+3$ и $2m+2\overline{p}+3$. Это означает, что расстояние между ними равняется $2\overline{p}$.

Из неравенства (25) леммы 6 имеем $P_1(2m+3) < 2m+3+2p(m) = 2m+$ $+3+2\overline{p}$, что противоречит предположению об отсутствии простых чисел на интервале $(2m+3, 2m+2\overline{p}+3)$. Отсюда получаем $P_1(2m+3) \le 2m+2\overline{p}+1 =$ $= 2(m+1)+2\overline{p}-1$.

Таким образом, справедливость неравенства (30) в этом случае доказана.

- $p(m+1) = \overline{p} > \overline{p}$. Гарантированная оценка для ближайшего простого числа, превышающего $2m+3$, будет иметь вид $P_1(2m+3) \le 2m+2\overline{p}-1 < 2m+2\overline{p}+1 \le$ $\le 2m+2\overline{p}-1$. Если число $2m+3$ не является простым, то $P_1(2m+1) =$ $= P_1(2m+2) = P_1(2m+3) \le 2m+2\overline{p}-1 < 2m+2\overline{p}+1 = 2(m+1)+2\overline{p}-1$ и неравенство (30) в этом случае доказано.

Пусть $2m+3$ — простое число. Проведя рассуждения, аналогичные первому случаю, получаем, что число $2m+2\overline{p}+3$ не может быть ближайшим простым числом, превышающим $2m+3$.

Следовательно, имеем $P_{-1}(2m+3) \ge 2m-2\overline{p}+5 > 2m-2\overline{p}+5$, что свидетельствует о справедливости неравенства (30).

Утверждение доказано.

Предложенное представление неотрицательных рациональных чисел $r(k, n)$, $k, n \in Z$, $0 \le r(k, n) \le 1$, введенные операции на последовательностях простых чисел специального вида и полученные оценки для границ интервалов, содержащих ближайшие простые числа, дают возможность обосновать методику для формализации и исследования величин меры принадлежности нечетких множеств, изложенную в [6].

Заключение

В настоящей работе рассмотрены специальные последовательности простых чисел, их свойства, введены операции на рассматриваемых последовательностях, получены оценки для интервалов размещения ближайших к заданному числу простых чисел. Предложен алгоритм для приближения произвольного рационального числа с помощью элементов введенных последовательностей простых чисел. Доказано, что решение, полученное с помощью предложенного алгоритма, является оптимальным решением рассматриваемой задачи приближения произвольного рационального числа. Рассмотрено множество неотрицательных рациональных чисел, которые представляются в виде отношения двух простых чисел из введенных последовательностей. Для этого множества получены нижнее и верхнее сопряженные множества, установлены соотношения между элементами различных множеств. Приведены и доказаны утверждения для оценок интервалов размещения ближайших к заданному целому простых чисел. Полученные результаты позволяют обосновать методику построения треугольных нечетких чисел в виде интервалов, границы которых выбираются с помощью элементов специальных последовательностей простых чисел, и были предложены в работе [6].

Є.В. Івохін, Д.О. Вадньов

ПРО ДЕЯКІ ВЛАСТИВОСТІ ТА ОЦІНКИ ДЛЯ ПОСЛІДОВНОСТЕЙ ПРОСТИХ ЧИСЕЛ

Розглянуто спеціальні послідовності простих чисел, їх властивості, введено операції на розглянутих послідовностях, отримано оцінки для інтервалів розміщення найближчих до заданого числа простих чисел. Запропоновано алгоритм для наближення довільного раціонального числа за допомогою елементів введених послідовностей простих чисел. Доведено твердження для оцінок інтервалів розміщення найближчих до заданого цілого простих чисел. Отримані результати дозволяють обгрунтувати методику побудови трикутних нечітких чисел у вигляді інтервалів, границі яких обираються за допомогою елементів спеціальних послідовностей простих чисел.

E V. Ivokhin, D.A. Vadnev

ON THE PROPERTIES AND ESTIMATES FOR THE PRIME NUMBERS SEQUENCES

The specific sequences of prime numbers, their properties, operations introduced on these sequences are considered. The estimates for arrangement intervals of the prime numbers the closest to the specified number are obtained. An algorithm to approximate an arbitrary rational number using elements of introduced sequences of primes is proposed. The statement for estimates of arrangement intervals of the closest to specified integer prime numbers. are proved. The obtained results enable us to substantiate the method of constructing triangular fuzzy numbers in the form of intervals the boundaries of which are selected using the members of special sequences of prime numbers.

1. *Нестеренко Ю.В.* Алгоритмические проблемы теории чисел. Введение в криптографию / Под ред. В.В. Ященко. — СПб. : Питер, 2001. — 288 с.
2. *Крэндалл Р., Померанс К.* Простые числа. Криптографические и вычислительные аспекты. — М. : Либроком, 2011. — 664 с.
3. *Генри С. Уоррен, мл.* Алгоритмические трюки для программистов. — М. : Вильямс, 2007. — 288 с.
4. *Iwaniec H.* On the error term in the linear sieve // ACTA Arithmetica. — 1971. — N 19. — P. 1–30.
5. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. — М. : МЦНМО, 2003. — 328 с.
6. *Івохін Є.В.* Про застосування спеціальних множин простих чисел для визначення міри належності нечітких множин // Журнал обчислювальної та прикл. математики. — 2013. — № 4. — С. 1–8.

Получено 04.06.2015.

Статья представлена к публикации членом редколлегии чл.-корр. НАНУ А.А. Чикрием.