*В. А. Минаев*

# ОБ ИНТЕРВАЛЬНЫХ ОЦЕНКАХ РАСПРЕДЕЛЕНИЯ ПРОСТЫХ ЧИСЕЛ

Для решения многих задач, связанных с обеспечением информационной безопасности, защитой конфиденциальных данных, требуется оценка распределения простых чисел на тех или иных интервалах натурального ряда.

Обратимся к истории. В списке проблем, перечисленных Эдмундом Ландау — известным немецким математиком — в 1914 г. на Пятом Международном математическом конгрессе, значится третья проблема Ландау (гипотеза Лежандра). Эта гипотеза, утверждающая, что между $n^2$ и $(n+1)^2$, где $n$ — натуральное число, всегда найдется простое число, до сих пор не была доказана.

Докажем ее, опираясь на закономерности образования простых и составных чисел, принадлежащих множествам $\{6k \pm 1\}$, $k = 1,2,3,...$, которые приведены в работе [1].

Итак, известно, что во множествах $\{6k \pm 1\}$, $k = 1,2,3,...$, содержатся все простые числа кроме 2 и 3 [1]. В зависимости от того, в какое из множеств $\{6k+1\}$ или $\{6k-1\}$ входит простое число, будем называть его плюс-простым числом (ППЧ) или минус-простым числом (МПЧ). Помимо простых чисел в этих же множествах содержатся и составные числа, которые соответственно назовем минус-составные — МСЧ и плюс-составные числа — ПСЧ (данные термины введены в работе [2]).

Таким образом, множество простых чисел есть объединение:

вычитания из множества $\{6k+1\}$, $k = 1,2,3,...$, множества плюс-составных чисел;

вычитания из множества $\{6k-1\}$, $k = 1,2,3,...$, множества минус-составных чисел;

двухэлементного множества $\{2;3\}$.

## 1. Доказательство гипотезы Лежандра (третья проблема Ландау)

На любом интервале $(0,x)$ находится $\frac{x}{2}$ парных чисел (2,4,6,...), $\frac{x}{6}$ троичных чисел (3, 9, 15, ...). Отметим, что числа $2,3$, относясь, по определению, к простым числам, одновременно являются первыми в последовательностях парных и троичных чисел. Все остальные числа, что нетрудно показать, относятся к множествам $\{6k \pm 1\}$, $k = 1,2,3,...$, которые содержат простые $\pi(x)$, а также составные $c(x)$ числа.

Отсюда имеем следующее соотношение:

$$x = \frac{x}{2} + \frac{x}{6} + \pi(x) + c(x), \tag{1.1}$$

где $x$ — количество натуральных чисел от 0 до $x$, или

$$\frac{x}{3} = \pi(x) + c(x). \tag{1.2}$$

Обозначим через $\pi_1 = \pi(n^2)$ и $\pi_2 = \pi((n+1)^2)$ число простых чисел на интервалах $(0,n^2)$ и $(0,(n+1)^2)$ соответственно. Кроме того, обозначим $c_1 = c(n^2)$ и $c_2 = c\left((n+1)^2\right)$ число составных чисел из множеств $\{6k \pm 1\}$, $k = 1,2,3,...$, на тех же интервалах.

Применительно к интервалу $(0,n^2)$ соотношение (1.2) приобретет вид:

$$\frac{n^2}{3} = \pi(n^2) + c(n^2) = \pi_1 + c_1. \tag{1.3}$$

Соответственно на интервале $(0,(n+1)^2)$ соотношение (1.2) имеет вид:

$$\frac{(n+1)^2}{3} = \pi_2 + c_2. \tag{1.4}$$

Вычтем из соотношения (1.4) соотношение (1.3):

$$\frac{(n+1)^2}{3}-\frac{n^2}{3}=\pi_2-\pi_1+c_2-c_1. \tag{1.5}$$

Отсюда имеем:

$$\frac{2n+1}{3}=\Delta\pi+\Delta c\ , \tag{1.6}$$

где $\Delta\pi=\pi_2-\pi_1;\ \Delta c=c_2-c_1$.

Очевидно, что третья проблема Ландау будет решена, если доказать, что для любого n

$$\Delta\pi>0, \tag{1.7}$$

или

$$\frac{2n+1}{3}-\Delta c>0, \tag{1.8}$$

иначе

$$\frac{2n+1}{3}+c_1-c_2>0. \tag{1.9}$$

В работе [1] показано, что составные числа с избыточной для деления на 6 единицей образуются с помощью соотношений:

$$C^+_{p_i^-}=p_i^-\cdot p_i^-+p_i^-\cdot 6m; \tag{1.10}$$

$$C^+_{p_i^+}=p_i^+\cdot p_i^++p_i^+\cdot 6m;m=0,1,2,3,...,\ i=1,2,3,... \tag{1.11}$$

Примеры ПСЧ, образованных от простых чисел 5, 7, 11, 13:

$\{25;55;85;...\}$

$\{49;91;133;...\}$

$\{121;187;253;...\}$

$\{169;247;325;...\}$

В (1.10) и (1.11) введены следующие обозначения:

$p_i^-$, $i=1,2,3,...$ – простое число из множества $\{6k-1\};k=1,2,3,...$, с недостающей единицей для деления нацело на 6 (МПЧ);

$p_i^+$, $i=1,2,3,...$ – простое число из множества $\{6k+1\};k=1,2,3,...$, с избыточной единицей для деления нацело на 6 (ППЧ).

Соответственно $C^+_{p_i^-}$ обозначает множество составных чисел, образуемое с помощью первого уравнения (1.10) и относящееся к множеству ПСЧ. Множество $C^+_{p_i^+}$, образуемое с помощью уравнения (1.11), также относится к множеству ПСЧ.

Нетрудно видеть из (1.10), что первое МПЧ (индекс $i=1$) образует на интервале $(0,n^2)$ число составных чисел из множества $\{6k+1\}$, $k=1,2,3,...$, равное

$$q_1^+=\left[\frac{n^2-p_1^-\cdot p_1^-}{6p_1^-}\right]+1^{1}. \tag{1.12}$$

[1] Здесь [ ] – обозначение целой части числа, введенное Гауссом.

Далее

$$q_2^+ = \left[\frac{n^2 - p_2^- \cdot p_2^-}{6p_2^-}\right] + 1 \quad (1.13)$$

...

$$q_{Q_1}^+ = \left[\frac{n^2 - p_{Q_1}^- \cdot p_{Q_1}^-}{6p_{Q_1}^-}\right] + 1, \quad (1.14)$$

где $p_{Q_1}^-$ — максимальное из МПЧ на интервале $(0, n^2)$, образующее ПСЧ на этом же интервале.

Добавочная единица образуется в (1.12)—(1.14) за счет первого составного числа, равного квадрату МПЧ.

Складывая (1.12)—(1.14), имеем:

$$Q_1^+ = \sum_{i=1}^{Q_1}\left(\left[\frac{n^2 - p_i^- \cdot p_i^-}{6p_i^-}\right] + 1\right) = \sum_{i=1}^{Q_1} q_i^+ ;\ i = 1,2,3,\ldots, \quad (1.15)$$

где $Q_1$ — индекс максимального МПЧ, образующего ПСЧ на интервале $(0, n^2)$ с помощью уравнения (1.10).

Аналогично ППЧ (простые числа с избыточной единицей) образуют на том же интервале $(0, n^2)$ следующее количество ПСЧ:

$$Q_2^+ = \sum_{i=1}^{Q_2}\left(\left[\frac{n^2 - p_i^+ \cdot p_i^+}{6p_i^+}\right] + 1\right); i = 1,2,3,\ldots, \quad (1.16)$$

где $Q_2$ — индекс максимального ППЧ, образующего ПСЧ на интервале $(0, n^2)$ с помощью уравнения (1.11).

Составные числа из множества $\{6k-1\}$, $k = 1,2,3,\ldots$, с недостающей единицей для деления на 6 (МСЧ) нацело образуются следующим образом от МПЧ и ППЧ [1]:

$$C_{p_i^-}^- = p_i^- \cdot p_i^+ + p_i^- \cdot 6m; \quad (1.17)$$

$$C_{p_i^+}^- = p_i^+ \cdot p_i^- + p_i^+ \cdot 6m; m = 0,1,2,3,\ldots,\ i = 1,2,3,\ldots \quad (1.18)$$

Примеры МСЧ, образованных от простых чисел 5 и 7; 7 и 5; 11 и 13; 13 и 11:

$\{35;65;95;\ldots\}$

$\{35;77;119;\ldots\}$

$\{143;209;275;\ldots\}$

$\{143;221;299;\ldots\}$

Отметим важный для доказательства практический результат — последовательности (1.17) и (1.18) для одинаковых $p_i^+, p_i^-$ не только начинаются одним составным числом, равным произведению $p_i^+ \cdot p_i^-$, но и через период, равный $6p_i^+ \cdot p_i^-$, также имеют одинаковые члены. Будучи распространенным на другие последовательности составных чисел вида $\{6k \pm 1\}$, $k = 1,2,3,\ldots$, данный результат дал возможность учесть эффект «пересечений» последовательностей.

Для последовательностей (1.17) и (1.18) по аналогии с (1.12)—(1.14) имеем:

$$q_1^- = \left[\frac{n^2 - p_1^- \cdot p_1^+}{6p_1^-}\right] + 1\ ;$$

$$q_2^- = \left[\frac{n^2 - p_2^- \cdot p_2^+}{6p_2^-}\right] + 1$$

...

$$q_{Q_3}^- = \left[\frac{n^2 - p_{Q_3}^- \cdot p_{Q_3}^+}{6p_{Q_3}^-}\right] + 1\cdot \tag{1.19}$$

Тогда аналогично выражениям (1.15) и (1.16) имеем:

$$Q_3^- = \sum_{i=1}^{Q_3}\left(\left[\frac{n^2 - p_i^- \cdot p_i^+}{6p_i^-}\right] + 1\right) = \sum_{i=1}^{Q_s} q_i^-;\ i = 1,2,3,..., \tag{1.20}$$

где $Q_3$ — индекс максимального МПЧ, образующего МСЧ на интервале $(0, n^2)$ с помощью соотношения (1.17).

Наконец, для механизма образования МСЧ, описанного уравнением (1.18), имеем:

$$Q_4^- = \sum_{i=1}^{Q_4}\left(\left[\frac{n^2 - p_i^+ \cdot p_i^-}{6p_i^+}\right] + 1\right);\ i = 1,2,3,...\ , \tag{1.21}$$

где $Q_4$ — индекс максимального ППЧ, образующего МСЧ на интервале $(0, n^2)$ с помощью соотношения (1.18).

Таким образом, общее количество составных чисел вида $\{6k \pm 1\}$, $k = 1,2,3...$, образованных на интервале $(0, n^2)$, равно:

$$c_1 = Q_1^+ + Q_2^+ + Q_3^- + Q_4^-. \tag{1.22}$$

Сложим уравнения (1.15), (1.16), (1.20), (1.21):

$$\begin{aligned} c_1 = &\sum_{i=1}^{Q_1}\left(\left[\frac{n^2 - p_i^- \cdot p_i^-}{6p_i^-}\right] + 1\right) + \sum_{i=1}^{Q_2}\left(\left[\frac{n^2 - p_i^+ \cdot p_i^+}{6p_i^+}\right] + 1\right) + \\ &+ \sum_{i=1}^{Q_3}\left(\left[\frac{n^2 - p_i^- \cdot p_i^+}{6p_i^-}\right] + 1\right) + \sum_{i=1}^{Q_4}\left(\left[\frac{n^2 - p_i^+ \cdot p_i^-}{6p_i^+}\right] + 1\right); i = 1,2,3,... \end{aligned} \tag{1.23}$$

Аналогичным образом находим выражение для $c_2$:

$$\begin{aligned} c_2 = &\sum_{i=1}^{Q_5}\left(\left[\frac{n^2 + 2n + 1 - p_i^- \cdot p_i^-}{6p_i^-}\right] + 1\right) + \sum_{i=1}^{Q_6}\left(\left[\frac{n^2 + 2n + 1 - p_i^+ \cdot p_i^+}{6p_i^+}\right] + 1\right) + \\ &+ \sum_{i=1}^{Q_7}\left(\left[\frac{n^2 + 2n + 1 - p_i^- \cdot p_i^+}{6p_i^-}\right] + 1\right) + \sum_{i=1}^{Q_8}\left(\left[\frac{n^2 + 2n + 1 - p_i^+ \cdot p_i^-}{6p_i^+}\right] + 1\right); \\ &i = 1,2,3,... \end{aligned} \tag{1.24}$$

где $Q_5$, $Q_6$, $Q_7$ и $Q_8$ — максимальные значения индекса простых чисел МПЧ и ППЧ, принадлежащих интервалу $(0,(n+1)^2)$ и с помощью соотношений (1.17) и (1.18) образующих на нем же множества МСЧ.

Так как интервал $(0, n^2)$ содержится в интервале $(0,(n+1)^2)$:

$c_2 = c_1 + \Delta c$,

где $\Delta c$, как определено ранее, — количество составных чисел вида $\{6k \pm 1\}$, $k = 1,2,3,...$, на интервале $(n^2,(n+1)^2)$.

Легко показать, что как на интервале $(0,n^2)$, так и на интервале $(0,(n+1)^2)$ составные числа, принадлежащие множествам $\{6k\pm1\}$, $k=1,2,3,\ldots$, образуются с помощью соотношений (1.10)—(1.11) и (1.17)—(1.18) за счет одних и тех же простых чисел (МПЧ и ППЧ), относящихся к интервалу $(0,n)$. Причем первые члены названных последовательностей либо меньше $n^2$, либо для последовательностей (1.10)—(1.11) равны $n^2$. Внутри интервалов $(n^2,(n+1)^2)$ могут относительно редко начинаться только последовательности МСЧ, т. е. (1.17)—(1.18). И этим эффектом при достаточно больших $n$ можно пренебречь, так как нетрудно показать, что внутри таких интервалов образуется только первый член соответствующих МСЧ, остальные выходят за верхнюю границу интервала, равную $(n+1)^2$. Например, внутри интервала ($5^2$ — $6^2$) образуется МСЧ, равное $5\cdot7=35$, а на интервале ($11^2$ — $12^2$) — МСЧ, равное $11\cdot13=143$, на интервале ($17^2$ — $18^2$) — МСЧ, равное $17\cdot19=323$ и т. д.

Покажем, что наибольшее простое число, образующее ПСЧ на интервале $(0,n^2)$, должно быть не более $n$. На самом деле, наибольшее ПСЧ вида $\{6k\pm1\}$, $k=1,2,3,\ldots$, не должно превышать $n^2$. Следующее число $n+1$, возведенное в квадрат, находится на верхней границе интервала $(n^2,(n+1)^2)$. Таким образом, внутрь интервала $(n^2,(n+1)^2)$ не попадают ПСЧ вида $\{6k\pm1\}$, образованные простыми числами, превышающими $n$. При этом учитывается, что разница между соседними простыми числами — не менее двух (для простых чисел — «близнецов»). А $(n+2)^2$ уже находится за верхней границей интервала $(0,(n+1)^2)$.

Из приведенных рассуждений очевидно, что $Q_1=Q_5;\ Q_2=Q_6;\ Q_3=Q_7;\ Q_4=Q_8$.

Найдем разность (1.24) и (1.23):

$$\Delta c=c_2-c_1.$$

Исходя из (1.8) очевидно, что с увеличением оценочного значения $\Delta c$ в результате различных допущений окончательный положительный вывод о доказательстве гипотезы Лежандра усиливается. Этим обстоятельством мы воспользуемся в процессе решения проблемы.

Итак, вычитая из (1.24) соотношение (1.23), имеем:

$$\begin{aligned}\Delta c=&\sum_{i=1}^{Q_1}\left(\left[\frac{n^2+2n+1-p_i^-\cdot p_i^-}{6p_i^-}\right]+1-\left[\frac{n^2-p_i^-\cdot p_i^-}{6p_i^-}\right]-1\right)+\\&+\sum_{i=1}^{Q_2}\left(\left[\frac{n^2+2n+1-p_i^+\cdot p_i^+}{6p_i^+}\right]+1-\left[\frac{n^2-p_i^+\cdot p_i^+}{6p_i^+}\right]-1\right)+\\&+\sum_{i=1}^{Q_3}\left(\left[\frac{n^2+2n+1-p_i^-\cdot p_i^+}{6p_i^-}\right]+1-\left[\frac{n^2-p_i^-\cdot p_i^+}{6p_i^-}\right]-1\right)+\\&+\sum_{i=1}^{Q_4}\left(\left[\frac{n^2+2n+1-p_i^+\cdot p_i^-}{6p_i^+}\right]+1-\left[\frac{n^2-p_i^+\cdot p_i^-}{6p_i^+}\right]-1\right)\end{aligned}\qquad(1.25)$$

С учетом того, что разность целой части от двух действительных положительных чисел $x_2$ и $x_1$ при $x_2\ge x_1$ больше или равна целой части от разности этих же чисел:

$$[x_2]-[x_1]\le[x_2-x_1],\qquad(1.26)$$

из (1.25) имеем:

$$\Delta c\le\Delta c_1=\sum_{i=1}^{Q_1}\left[\frac{2n+1}{6p_i^-}\right]+\sum_{i=1}^{Q_2}\left[\frac{2n+1}{6p_i^+}\right]+\sum_{i=1}^{Q_3}\left[\frac{2n+1}{6p_i^-}\right]+\sum_{i=1}^{Q_4}\left[\frac{2n+1}{6p_i^+}\right].\qquad(1.27)$$

Далее, учитывая, что:

$$[x_1]+[x_2]\le[x_1+x_2], \tag{1.28}$$

а также, что $Q_3 \cong Q_1$ и $Q_4 \cong Q_2$, получим:

$$\Delta c \le \Delta c_1 \le \Delta c_2 = 2\left(\sum_{i=1}^{Q_1}\frac{2n+1}{6p_i^-}+\sum_{i=1}^{Q_2}\frac{2n+1}{6p_i^+}\right). \tag{1.29}$$

Для удобства доказательства далее будем рассматривать множества простых чисел МПЧ и ППЧ как единое множество:

$$\{p_i\}=\{p_i^-\}+\{p_i^+\}, i=1,2,3,... \tag{1.30}$$

Определим $M = Q_1 + Q_2$ как индекс максимального простого числа из объединенного множества (1.30), которое образует составные числа вида $\{6k \pm 1\}$, $k = 1,2,3...$, на интервале $(0,(n+1)^2)$.

Тогда (1.29) преобразуется к виду:

$$\Delta c_2 = \frac{2n+1}{3}\sum_{i=1}^{M}\frac{1}{p_i}\cdot \tag{1.31}$$

Введем обозначение:

$$z(M)=\sum_{i=1}^{M}\frac{1}{p_i}\cdot \tag{1.32}$$

Как было отмечено, последовательности МСЧ и ПСЧ, образуемые с помощью соотношений (1.10)–(1.11) и (1.17)–(1.18), периодически «пересекаются», т. е. имеют одинаковые элементы.

Покажем это, например, приравняв (1.17) и (1.18):

$$p_i^- \cdot p_i^+ + p_i^- \cdot 6k = p_i^+ \cdot p_i^- + p_i^+ \cdot 6l; i = 1,2,3,...; k,l = 0,1,2,3... \tag{1.33}$$

Отсюда

$$p_i^- k = p_i^+ l, \tag{1.34}$$

т. е. совпадение элементов последовательностей (1.17) и (1.18) происходит при $k = p_i^+$ и $l = p_i^-$.

Таким образом, период равенства элементов последовательностей (1.17) и (1.18) равен $6p_i^- \cdot p_i^+$.

Из-за совпадения ряда элементов последовательностей именно на количество «пересекающихся» составных чисел вида $\{6m-1\}; m = 1,2,3...$, уменьшается общее количество составных чисел на интервале $(n^2,(n+1)^2)$.

Отметим, что эффект взаимосвязи последовательностей, образующих МСЧ и ПСЧ, впервые описан в настоящей статье. Вследствие данного эффекта несколько корректируется представление о «древе жизни», иллюстрирующем в работе [1] структуру натурального ряда. Согласно данному эффекту, некоторые листья — составные числа — через определенный период должны одновременно принадлежать разным ветвям «дерева».

Рассмотрим все возможные «пересечения» последовательностей, формирующих составные числа на интервале $(n^2,(n+1)^2)$.

«Пересечения» ПСЧ, формирующихся с помощью соотношений (1.10)–(1.11), определяются уравнениями:

$$\begin{aligned}
&p_i^- \cdot p_i^- + p_i^- \cdot 6m = p_j^- \cdot p_j^- + p_j^- \cdot 6l\\
&p_i^+ \cdot p_i^+ + p_i^+ \cdot 6m = p_j^+ \cdot p_j^+ + p_j^+ \cdot 6l\\
&p_i^+ \cdot p_i^+ + p_i^+ \cdot 6m = p_j^- \cdot p_j^- + p_j^- \cdot 6l\\
&p_i^- \cdot p_i^- + p_i^- \cdot 6m = p_j^+ \cdot p_j^+ + p_j^+ \cdot 6l,
\end{aligned} \tag{1.35}$$

где $i, j = 1,2,3,...M; m, l = 0,1,2,...$

Вторая система уравнений, определяющих «пересечения» МСЧ, записывается в виде:

$$\begin{aligned} p_i^- \cdot p_i^+ + p_i^- \cdot 6m &= p_j^- \cdot p_j^+ + p_j^- \cdot 6l \\ p_i^+ \cdot p_i^- + p_i^+ \cdot 6m &= p_j^+ \cdot p_j^- + p_j^+ \cdot 6l \\ p_i^- \cdot p_i^+ + p_i^- \cdot 6m &= p_j^+ \cdot p_j^- + p_j^+ \cdot 6l \\ p_i^+ \cdot p_i^- + p_i^+ \cdot 6m &= p_j^- \cdot p_j^+ + p_j^- \cdot 6l, \end{aligned} \tag{1.36}$$

где $i, j = 1,2,3,...M; m, l = 0,1,2,...$

Приведем множества МПЧ и ППЧ к единой нумерации:

$p_1 = 5, p_2 = 7, p_3 = 11, p_4 = 13$ и т. д.

Нетрудно показать, что для общего случая период, через который в последовательностях (1.35)—(1.36) возникают «пересечения», равен

$$T(p_i, p_j) = 6 p_i p_j; i, j = 1,2,...M. \tag{1.37}$$

Общее количество составных чисел, по аналогии с (1.15), (1.16), (1.20), (1.21), совпадающих по своему значению в двух разных последовательностях на интервалах $(0, n^2)$ и $(0,(n+1)^2)$, равно:

$$q_1 = \sum_{i=1}^{M} \left\{ \left[ \frac{(n+1)^2 - p_i \cdot p_j}{6 p_i \cdot p_j} \right] + 1 \right\}; \tag{1.38}$$

$$q_2 = \sum_{i=1}^{M} \left\{ \left[ \frac{n^2 - p_i \cdot p_j}{6 p_i \cdot p_j} \right] + 1 \right\}; i, j = 1,2,3,...M. \tag{1.39}$$

Вычитая (1.39) из (1.38) и учитывая (1.26), оценим общее количество «пересекающихся» составных чисел на интервале $(n^2,(n+1)^2)$:

$$\Delta q \cong \frac{1}{2} \cdot \frac{2(2n+1)}{6} z^2 = \frac{2n+1}{6} z^2 \ , \tag{1.40}$$

где

$$z^2 = \sum_{i=1}^{M} \frac{1}{p_i} \cdot \sum_{j=1}^{M} \frac{1}{p_j}; i, j = 1,2,3...M. \tag{1.41}$$

Коэффициент $\frac{1}{2}$ введен для учета того, что необходимо рассмотреть только половину «пересечений», которая является дублем составных чисел вида $\{6k \pm 1\}; m = 1,2,3,...$ , на интервале $(n^2,(n+1)^2)$.

Кроме того, из (1.41) вычтем «самопересечения» типа $\frac{1}{p_i^2}; i = 1,2,...M.$

В результате имеем

$$\Delta\pi(n, p) = \frac{2n+1}{3} \cdot \left\{ 1 - z + \frac{z^2}{2} - \frac{\rho}{2} \right\}, \tag{1.42}$$

где

$$\rho = \sum_{i=1}^{M} \frac{1}{p_i^2} \tag{1.43}$$

или

$$\rho = \zeta_p(2) - \frac{1}{4} - \frac{1}{9}. \tag{1.44}$$

В соотношении (1.44) $\xi_p(2)$ — дзета-функция Римана на множестве простых чисел, равная:

$$\zeta_p(2)=\frac{1}{4}+\frac{1}{9}+\sum_{i=1}^{M}\frac{1}{p_i^2}.$$

Известно [3], что

$$\zeta_p(2)\to 0{,}453... \tag{1.45}$$

Соответственно, при $M\to\infty$

$$\rho\to 0{,}0919. \tag{1.46}$$

Преобразуем (1.42) к виду:

$$\Delta\pi(n,z)=\frac{2n+1}{6}\cdot\left\{(1-z)^2+(1-\rho)\right\} \tag{1.47}$$

Очевидно, что при любых z и n $\Delta\pi(n,z)>0$.

Таким образом, теорема Ландау доказана или гипотеза Лежандра подтверждена.

## 2. Некоторые следствия доказательства теоремы Ландау

*2.1. Простое доказательство гипотезы Бертрана*

В 1845 г. французским математиком Ж. Бертраном была выдвинута гипотеза, названная впоследствии постулатом, о том, что для любого натурального $n>1$ найдется простое число в интервале $(n,\ 2n)$. В 1845 г. эта гипотеза доказана русским математиком П. Л. Чебышевым в своей знаменитой теореме. Индийский математик С. Рамануджан в 1920 г. нашел более простое доказательство гипотезы Бертрана, а венгр П. Эрдёш — в 1932 г. еще более простое.

Используя доказательство теоремы Ландау, можно весьма просто обосновать справедливость постулата Бертрана.

Пусть

$$m=\sqrt{n}\ \text{ и }\ m+1=\sqrt{n}+1. \tag{2.1.1}$$

Тогда

$$(m+1)^2-m^2=n+2\sqrt{n}+1-n=2\sqrt{n}+1. \tag{2.1.2}$$

Покажем, при каких n справедливо соотношение:

$$2\sqrt{n}+1<n, \tag{2.1.3}$$

означающее, что интервал, используемый в постулате, шире и включает интервал между квадратами последовательных чисел натурального ряда в доказанной в настоящей работе теореме Ландау, всегда содержащий простое число.

Из (2.1.3) следует

$$0<n^2-6n+1,$$

или при нахождении корней квадратного уравнения,

$$\left(n-3+2\sqrt{2}\right)\left(n-3-2\sqrt{2}\right)>0. \tag{2.1.4}$$

Анализ (2.1.4) показывает, что постулат Бертрана всегда справедлив при $n>5$. Дополнительный анализ при $1<n<5$ свидетельствует о том, что названный постулат выполняется для всех $n>1$.

*2.2. Доказательство гипотезы Брокарда*

Из доказательства гипотезы Лежандра легко выводится утверждение, названное гипотезой Брокарда: между квадратами подряд идущих простых чисел, за исключением первых двух, всегда найдется хотя бы 4 простых числа.

Обозначим $\pi\left(p_{n+1}^2\right)$ число простых чисел на интервале $\left(0,p_{n+1}^2\right)$ и $\pi\left(p_n^2\right)$ — число простых чисел на интервал $\left(0,p_n^2\right)$. Где $p_n$ и $p_{n+1}$ — подряд идущие простые числа. Тогда гипотеза Брокарда формулируется как:

$$\Delta\pi_в=\pi\left(p_{n+1}^2\right)-\pi\left(p_n^2\right)\ge 4 \tag{2.2.1}$$

Пусть, без ограничения общности, $p_n^2 = n^2$.

Докажем (2.2.1) для простых чисел — «близнецов», когда расстояние между подряд идущими простыми числами $p_{n+1} - p_n = 2$ — минимально. В случае, когда соседние простые числа не «близнецы», доказательство очевидно.

Итак, вводя определение $\Delta_B$:

$$\Delta_B = (p_n + 2)^2 - p_n^2 = 4p_n + 4 = 4(n+1), \tag{2.2.2}$$

имеем

$$\Delta_B = 4n + 4 = 2(\Delta + 1), \tag{2.2.3}$$

т. е. $\Delta = 2n + 1$ включен в интервал $\Delta_B$.

Из (2.2.3) следует, что всегда $\Delta\pi_B > 0$, ибо на большем, чем $\Delta$, интервале, как было показано при доказательстве теоремы Ландау, всегда есть простое число.

Учитывая, что при $p_n^2 = n^2$ на интервале $(p_n^2, p_{n+1}^2)$ МСЧ и ПСЧ образуются такими же простыми числами, как и на интервале $(n^2, (n+1)^2)$, справедливо следующее соотношение:

$$\Delta_B = \frac{4(n+1)}{6}\{(1-z)^2 + (1-\rho)\}. \tag{2.2.4}$$

Покажем, что даже при минимуме выражения в фигурных скобках гипотеза Брокарда подтверждается.

На самом деле, минимум $(1-z)^2 = 0$, а минимум $(1-\rho) = 0{,}908$ достигается при максимуме $\rho = 0.0919$.

Тогда необходимо найти $n$, при котором выполняется неравенство

$$\frac{4(n+1)}{6} \cdot 0{,}908 \geq 4. \tag{2.2.5}$$

Очевидно, что при $n > 6$ неравенство (2.25) выполняется всегда.

Легко показать, что и при $n \geq 5$ гипотеза Брокарда справедлива, а небольшое завышение оценок здесь и при подтверждении постулата Бертрана связано с «краевыми эффектами», обусловленными началом формирования простых чисел в натуральном ряду.

*2.3. Решение проблемы «простых близнецов»*

Используя соотношение (2.2.4), покажем, что число «простых близнецов», т. е. простых чисел, разность между которыми равна 2, бесконечно. Для этого в выражении (2.2.4) вычтем количество простых чисел, равное количеству простых чисел вида $\{6k \pm 1\}, k = 1,2,3,...$, находившихся на интервале $(n^2, (n+1)^2)$. Тем самым мы учтем все простые числа, стоящие «против» составных чисел и потому не являющиеся «близнецами» простых. Здесь необходимо отметить, что «против» составных чисел могут также оказаться и другие составные. Таким образом, вычитая удвоенное количество составных, мы как бы искусственно занижаем количество простых чисел — «близнецов» на интервале $(n^2, (n+1)^2)$ путем учета уже учтенного.

Итак, оценка количества простых чисел — «близнецов» на интервале $(n^2, (n+1)^2)$ записывается в виде:

$$\Delta\pi_B(n,z) \geq \frac{2n+1}{3} \cdot \{1 - 2z + z^2 - \rho\}, \tag{2.3.1}$$

$$\Delta\pi_B(n,z) \geq \frac{2n+1}{3}\{(1-z)^2 - \rho\}. \tag{2.3.2}$$

Таким образом, при $n \to \infty$ количество простых чисел — «близнецов» $\Delta\pi_B \to \infty$, несмотря на то, что на коротком интервале $1 - \sqrt{\rho} < z < 1 + \sqrt{\rho}$ выражение в квадратных скобках становится отрицательным по причине упомянутого искусственного занижения.

В результате мы пришли к выводу о том, что число простых чисел — «близнецов» на интервале $(n^2, (n+1)^2)$ стремится к бесконечности при $n \to \infty$, тем самым решив вторую проблему Ландау о том, что число «простых близнецов» бесконечно.

В заключение отмечу, что практические расчеты содержания простых чисел, выполненные с использованием полученного соотношения (1.47), показали, что на начальном этапе формирования натурального ряда происходит занижение оценки количества простых чисел на интервалах $(n^2,(n+1)^2)$, а затем — завышение оценки их количества. Накопленные ошибки обусловлены оперированием с нецелочисленными функциями. Однако это свойство не является принципиальным для доказательства гипотезы Лежандра, а также для тех следствий, которые вытекают из приведенного доказательства.

Для практических расчетов количества простых чисел в интервале $(n^2,(n+1)^2)$ учтем, что целые числа в выражении (1.27) начинают образовываться со значений $n > 15$ (для минимального простого числа, образуемого во множестве $\{6k \pm 1\}$, $k = 1,2,3,\ldots$, равного 5), а «пересечения» по аналогичной формуле возникают после $n > 75$ (для минимального квадрата простых чисел, образуемых в том же множестве $\{6k \pm 1\}$, $k = 1,2,3,\ldots$, равного 25). Для этого отбросим соответствующее количество слагаемых в выражениях для z, квадрата z и ϱ.

В этом случае приближенная формула приобретает вид

$$\Delta\pi(n,z) = \frac{2n+1}{6} \cdot \left\{(1-z)^2 + 0{,}45\right\}. \qquad (2.3.3)$$

На рис. 1 приведен эмпирический график изменения количества простых чисел в интервале $(n^2,(n+1)^2)$ и для сравнения (пунктирная линия) — оценка их количества по формуле (2.3.3).

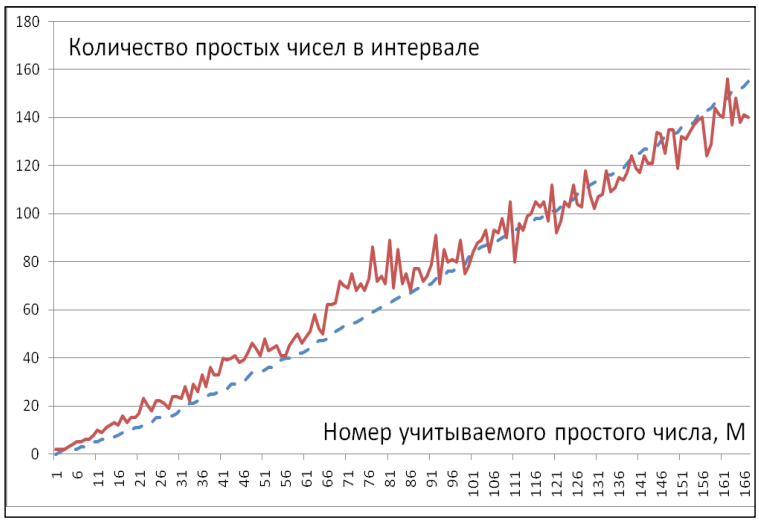


*Рис. 1.*

Таким образом, наблюдается хорошее согласование эмпирических данных и модели (2.3.3). При этом отмечается занижение оцененного количества простых чисел на некотором начальном интервале. Для точного согласования эмпирических и теоретических данных необходимо программно реализовать целочисленный вариант модели (1.47).

## СПИСОК ЛИТЕРАТУРЫ:

1. *Минаев В. А., Хренов В. П.* Фундаментальная закономерность формирования простых чисел и информационная безопасность // Безопасность информационных технологий. 2008. № 3. С. 20–32.
2. *Каленикова Н. А., Минаев В. А, Хренов В. П.* Улучшение метода Ферма: новый алгоритм факторизации // Безопасность информационных технологий. 2010. № 2. С. 76–79.
3. *Merrifield C. W.* The sums of the series of reciprocals of the prime numbers and of their powers // Proc. Roy. Soc. London. 1881. Vol. 33. P. 4–10.