Оценка интервальных распределений простых чисел как фундаментальный вклад в создание алгоритмов защиты информации*

***С.В. Клименко*[1], *В.А. Минаев*[2], *М.П. Сычев*[2]**
stanislav.klimenko@gmail.com|m1va@yandex.ru|runc@busts.ru
Протвино, [1]Институт физико-технической информатики
Московский физико-технический институт (государственный университет)
[2]Московский государственный университет им. Н.Э. Баумана

В работе, исходя из оценки количества составных чисел вида $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$, на интервале $(0, n)$, приведено новое соотношение для оценки количества простых того же вида на указанном интервале. Исходя из данного соотношения, доказаны гипотезы Лежандра, Брокарда и Бертрана. Делается вывод, что полученные интервальные оценки могут улучшить алгоритмы обеспечения информационной безопасности, шифрования/дешифрования информации, в которых используются простые числа.

Ключевые слова: *простые числа, составные числа, интервальные гипотезы, алгоритмы поиска простых чисел, защита информации*

Estimation of Prime Interval Distributions as a Fundamental Contribution in the Creation of Algorithms for Information Security*

***S.V. Klimenko*[1], *V.A. Minaev*[2], *M.P. Sychev*[2]**
Protvino, [1]Institute of Computing for Physics and Technology
Moscow Institute of Physics and Technology (State University)
[2]Bauman Moscow State Technical University

Using the estimation of composite numbers quantity type $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$, on an interval $(0, n)$, the new ratio for assessment in the specified interval of quantity primes the same type is given. Proceeding from this ratio, hypotheses of Legendre, Brokard and Bertrand are proved. It is concluded that received interval estimates can improve algorithms of ensuring information security, coding and decoding of information in which prime numbers are used.

Keywords: *prime numbers, composite numbers, interval hypotheses, algorithms of prime numbers searching, information security*

Введение

Проблемы оценки распределения простых чисел и их поиска являются актуальными со времен Евклида [1, 2, 3, 4, 5, 6, 7, 8].

Формальные соотношения, описывающие механизмы формирования составных чисел вида $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$, представленные в работе [9], позволили обосновать и реализовать новые, более производительные алгоритмы вычисления простых чисел на любом интервале натурального ряда [10, 11, 12], а также доказать гипотезы Лежандра, Брокарда, подтвердить постулат Бертрана и подойти к решению других интервальных задач [9]. Полученные интервальные оценки направлены на улучшение алгоритмов обеспечения информационной безопасности, шифрования/дешифрования информации, где используются простые числа [13].

В работе [9] показано, что количество простых чисел на интервале $(0, n)$ оценивается как:

$$\pi(n) = \frac{n}{6}\left[(1 - z') + (1 - \rho') + \frac{1}{3}\left(1 - \frac{z'}{2}\right)\right], \quad (1)$$

где $z' = \sum_{i=1}^{L} \frac{1}{p_i}$; $\rho' = \sum_{i=1}^{L} \frac{1}{p_i^2}$; p_i – простые числа вида $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$; в количестве L, участвующие в формировании составных чисел вида $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$ на интервале $(0, n)$.
Выражение ρ' для представим в виде:

$$\rho' = \xi_p(2) - \frac{1}{4} - \frac{1}{9}, \quad (2)$$

где $\xi_p(2)$ – дзета-функция Римана на множестве простых чисел.
Известно, что при

$$\xi_p(2) \to 0.453\ldots \text{ при } L \to \infty. \quad (3)$$

Соответственно, учитывая (2)

$$\rho' \to 0.092$$
$$1 - \rho' \to 0.908. \quad (4)$$

Работа выполнена и опубликована при финансовой поддержке РФФИ, гранты 16-07-20854, 16-37-10489

Используя определение дзета-функций Римана на множестве простых чисел, представим (1) в виде:

$$\pi(n) = \frac{n}{6}[(1.833\ldots - \zeta_p(1))^2 + \\ +(1.361\ldots - \zeta_p(2)) + \frac{2}{3}(2.833\ldots - \zeta_p(1))] \quad (5)$$

Интервальных гипотезы

Гипотеза Лежандра

Гипотеза Лежандра (третья проблема Ландау) утверждает, что между n^2 и $(n+1)^2$ всегда найдется простое число. Докажем ее, опираясь на соотношение (1), приводящееся в [9] к виду:

$$\pi(n)\frac{n}{3}\left[1 - z' + \frac{z'^2}{2} - \frac{\rho'}{2}\right] + 2L^2 - \\ -L(L+1)\cdot z' + \frac{1}{3}L. \quad (6)$$

Вводя обозначения:

$$G(z') = 1 - z' + \frac{z'^2}{2} - \frac{\rho'}{2} = \\ = \frac{1}{2}\left[(1-z')^2 + (1-\rho')\right] \quad (7)$$

и учитывая оценку из [10] для $L \simeq \frac{\sqrt{n}}{6}$, получим:

$$\pi[(n+1)^2] = \frac{(n+1)^2}{3}\cdot G(z') + \frac{2(n+1)^2}{36} - \\ -\frac{(n+1)^2}{36}z' - \frac{n+1}{6}z' + \frac{1}{3}\cdot\frac{n+1}{6} \quad (8)$$

$$\pi\left[(n)^2\right] = \frac{n^2}{3}\cdot G(z') + \frac{2n^2}{36} - \\ -\frac{n^2}{36}z' - \frac{n}{6}z' + \frac{1}{3}\cdot\frac{n}{6}. \quad (9)$$

Нетрудно показать, что $G(z')$ и z' образуются одними и теми же простыми числами, максимальное из которых не превышает $n+1$. Вычитая (9) из (8), получаем количество простых чисел между n^2 и $(n+1)^2$:

$$\triangle\pi_L = \pi\left[(n+1)^2\right] - \pi\left[(n)^2\right] = \\ = \frac{2n+1}{3}G(z') + \frac{2n+1}{18} - \frac{2n+1}{36}z' - \frac{z'}{6} + \frac{1}{18} = \\ = \frac{2n+1}{3}G(z') + \frac{n}{9} + \frac{1}{9} - \frac{7}{36}z' - \frac{nz'}{18}. \quad (10)$$

Или при $n \to \infty$

$$\triangle\pi_L \cong \frac{n}{3}\left[(1-z')^2 + (1-\rho') + \frac{1}{3}\left(1 - \frac{z'}{2}\right)\right] \quad (11)$$

Нетрудно показать, что выражение в квадратных скобках всегда больше нуля. Таким образом, третья проблема Ландау решена, и гипотеза Лежандра доказана.

На рис. 1 приведена модельная (сплошная линия) и эмпирическая зависимость (кружки) количества простых чисел в интервале $(n^2, (n+1)^2)$ – ось ординат) от n – ось абсцисс. Очевидно хорошее согласование данных (квадрат коэффициента корреляции теоретических и эмпирических данных равен 0,996).

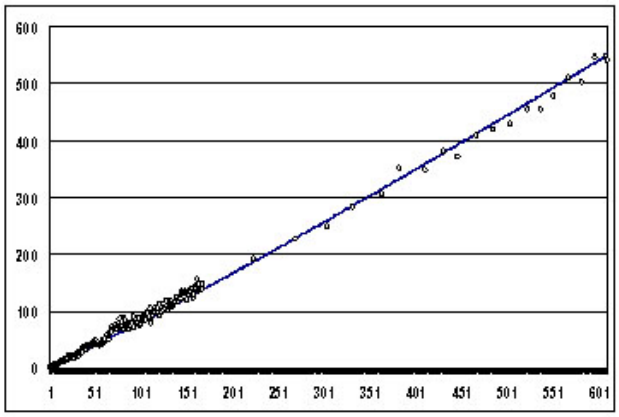

Рис. 1: Моделирование распределения простых чисел в интервале $(0, (n+1)^2)$

Гипотеза Бертрана

В 1845 году Ж. Бертраном выдвинута гипотеза, названная впоследствии постулатом, о том, что для любого натурального $n > 1$ найдётся простое число в интервале $(n, 2n)$. В 1845 году эта гипотеза доказана русским математиком П.Л. Чебышевым в своей знаменитой теореме.

Индийский математик С. Раманаджан в 1920 году нашёл более простое доказательство гипотезы Бертрана, а венгр П. Эрдёш – в 1932 году ещё более простое. Используя доказательство гипотезы Лежандра, можно весьма просто обосновать справедливость постулата Бертрана.

Пусть

$$m = \sqrt{n} \quad \text{и} \quad m + 1 = \sqrt{n} + 1 \quad (12)$$

Тогда

$$(m+1)^2 - m^2 = 2\sqrt{n} + 1 \quad (13)$$

Покажем, при каких справедливо соотношение:

$$2\sqrt{n} + 1 < n, \quad (14)$$

означающее, что интервал, используемый в постулате, шире и включает интервал между квадратами последовательных чисел натурального ряда в

решенной в [9] проблеме Ландау, всегда содержащий простое число.
Из (14) следует

$$0 < n^2 - 6n + 1 = (n - 3 + 2\sqrt{2})(n - 3 - 2\sqrt{2}) \tag{15}$$

Анализ выражения (15) показывает, что постулат Бертрана всегда справедлив при $n > 6$. Простой дополнительный анализ при $1 < n \leqslant 6$ свидетельствует о том, что названный постулат выполняется для всех $n > 1$.

Гипотеза Брокарда

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

Обозначим $\pi(p_{i+1}^2)$ число простых чисел в интервале $(0, p_{i+1}^2)$ и $\pi(p_i^2)$ – число простых чисел в интервале $(0, p_i^2)$. Где p_i и p_{i+1} – подряд идущие простые числа. Тогда гипотеза Брокарда формулируется как:

$$\triangle\pi_B = \pi(p_{i+1}^2) - \pi(p_n^2) \geqslant 4 \tag{16}$$

Пусть $p_n^2 = m^2$.

Докажем справедливость соотношения (16) для простых чисел – «близнецов», когда расстояние между подряд идущими простыми числами $p_{i+1} - p_i = 2$ – минимально. В случае, когда соседние простые числа не «близнецы», доказательство очевидно.

Итак, вводя определение $\triangle_B$:

$$\triangle_B = (p_i + 2)^2 - p_i = 4p_i + 4 = 4(m + 1), \tag{17}$$

имеем

$$\triangle_B = 4m + 4 = 2(\triangle + 1) \tag{18}$$

т.е. $\triangle = 2m + 1$ включен в интервал $\triangle_B$.

Из (18) следует, что $\triangle\pi_B$ всегда больше 0, ибо на большем, чем $\triangle$ интервале, как было показано при доказательстве гипотезы Лежандра, всегда есть простое число.

Учитывая [9], что при $p_i^2 = m^2$ на интервале (p_i^2, p_{i+1}^2) составные числа $\{6k \pm 1\}, r = 1, 2, 3, \ldots,$ образуются такими же простыми числами, как и на интервале $(m^2, (m + 1)^2)$, справедливо следующее соотношение:

$$\triangle\pi_B = \frac{4(m+1)}{6}\{(1 - z')^2 + (1 - \rho') + \frac{1}{3}(1 - \frac{z'}{2})\} \tag{19}$$

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

На самом деле, минимум выражения

$$(1 - z')^2 + \frac{1}{3}\left(1 - \frac{z'}{2}\right) = 1.026,$$

а минимум $(1 - \rho') = 0.908$ достигается при максимуме $\rho' = 0.0919$.

Тогда необходимо найти m, при котором выполняется неравенство

$$\frac{4(m+1)}{6}(0.908 + 1.026) \geqslant 4 \tag{20}$$

Очевидно, что при $n \geqslant 5$, неравенство (20), а значит и (16) выполняется всегда. Таким образом, гипотеза Брокарда подтверждена.

Заключение

Найденное в [9] новое, более точное соотношение для оценки количества простых чисел, содержащихся в интервале $(0, n)$, дало возможность решить открытую проблему математики – доказать гипотезу Лежандра, а также доказать гипотезу Брокарда и по-новому подойти к подтверждению постулата Бертрана, что выступает фундаментальным достижением как в области математики, так и в области разработки вычислительных процедур в сфере обеспечения информационной безопасности.

Литература

[1] Начала Евклида. Перевод с греческого и комментарии Д.Д. Мордухай-Болтовского при редакционном участии И.Н. Веселовского и М.Я. Выгодского. М.-Л.: ГТТИ, 1949–1951. 446 с.

[2] Чебышев П.Л. Избранные математические труды / Ответственный редактор И.М. Виноградов. Редактор-составитель А.О. Гельфонд. М.: - Ленинград: ОГИЗ Гостехиздат, 1946. 200 с.

[3] Виноградов И.М. Некоторое общее свойство распределения простых чисел // Математический сборник. 1940. Т. 7(49). Вып. 2. С. 365–372.

[4] Бараш Л.Ю. Алгоритм AKS проверки чисел на простоту и поиск констант генераторов псевдослучайных чисел // Безопасность информационных технологий. 2005. Вып. 2. С. 27–38.

[5] Карацуба А.А. Об асимптотической формуле Римана для $\pi(x)$ // Доклады РАН. 2004. Т. 396, № 5. С. 595–596.

[6] Atkin A.O.L., Bernstein D.J. Prime sieves using binary quadratic forms // Math. Comp. 2003. № 73 (246), pp. 1023–1030.

[7] Crandall R., Pomerance C. Prime Numbers: A Computational Perspective. M.: Springer New York, 2005. 597 c.

[8] Tolev D.I., Additive Problems with Prime Numbers of Special Type. Acta Arithmetica, 96, 1 (2000). Pp. 53–88.

[9] Минаев В.А. Простые числа: новый взгляд на закономерности формирования. М.: Издательский дом «Логос», 2011. 80 с.

[10] Минаев В.А. Теорема о полном множестве простых чисел // Книжная серия журнала «Безопасность информацион-ных технологий». М.: НИЯУ МИФИ, 2011. 24 с.

[11] Минаев В.А., Сычев М.П., Никонов С.А., Никеров Д.В. Реализация индекс-ных алгоритмов поиска простых чисел с помощью параллельных вычислений // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2015. № 6. С.82-90.

[12] Минаев В.А., Сычев М.П., Никонов С.А., Никеров Д.В. Модели и алгоритмы поиска простых чисел. М.: Издательство «РТСофт» – «Космоскоп», 2016. 176 с.

[13] Нечаев В.И. Элементы криптографии. Основы теории защиты информации. М.: Высшая школа, 1999. 109 с.

[14] Карацуба А.А., Королев М.А. Аргумент дзета-функции Римана // Успехи математических наук. 2005. Т. 60, №3 (363). С. 41–96.