Постулат Бертрана

Глава 2

Мы видели, что последовательность простых чисел $2, 3, 5, 7, \ldots$ бесконечна. Чтобы показать, что размеры лакун (промежутков между соседними числами) в ней не ограничены, обозначим через

$$N = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p$$

произведение всех простых чисел, которые меньше $k + 2$. Заметим, что ни одно из k чисел

$$N + 2, N + 3, N + 4, \ldots, N + k, N + (k + 1)$$

не является простым, так как простые делители любого числа $i = 2, 3, \ldots, k + 1$ меньше $k + 2$ и делят N; следовательно, они делят также $N + i$. С помощью этого приема мы находим, например, для $k = 10$, что ни одно из чисел

$$2312, 2313, 2314, \ldots, 2321$$

не является простым.

Существуют также верхние оценки для лакун в последовательности простых чисел. Согласно самой известной оценке, «лакуна до следующего простого не может быть больше числа, с которой она начинается». Это утверждение называют постулатом Бертрана, так как оно было высказано в форме предположения и проверено эмпирически для $n < 3\,000\,000$ Джозефом Бертраном. Впервые оно было доказано Пафнутием Чебышёвым около 1850 года [5*]. Значительно более простое доказательство нашел индийский гений Рамануджан. Доказательство в нашей книге принадлежит Паулю Эрдёшу. Оно взято из его первой статьи [1], опубликованной в 1932 году, когда Эрдёшу было 19 лет.

Постулат Бертрана.
Для каждого $n \geq 1$ существует такое простое число p, что $n < p \leq 2n$.

■ **Доказательство.** Мы получим достаточно хорошую оценку биномиального коэффициента $\binom{2n}{n}$ и с ее помощью покажем, что если бы он не имел простых делителей p, лежащих между n и $2n$, то он был бы «слишком мал». Наше рассуждение состоит из пяти шагов.

(1) Вначале докажем постулат Бертрана для $n < 4000$. Для этого нет необходимости проверять 4000 вариантов: достаточно (используя «прием Ландау») проверить, что

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$

Джозеф Бертран

Beweis eines Satzes von Tschebyschef.

Von P. Erdös in Budapest.

Für den zuerst von Tschebyschef bewiesenen Satz, laut dessen es zwischen einer natürlichen Zahl und ihrer zweifachen stets wenigstens eine Primzahl gibt, liegen in der Literatur mehrere Beweise vor. Als einfachsten kann man ohne Zweifel den Beweis von Ramanujan[1]) bezeichnen. In seinem Werk *Vorlesungen über Zahlentheorie* (Leipzig, 1927), Band I, S. 66—68 gibt Herr Landau einen besonders einfachen Beweis für einen Satz über die Anzahl der Primzahlen unter einer gegebenen Grenze, aus welchem unmittelbar folgt, daß für ein geeignetes q zwischen einer natürlichen Zahl und ihrer q-fachen stets eine Primzahl liegt. Für die augenblicklichen Zwecken des Herrn Landau kommt es nicht auf die numerische Bestimmung der im Beweis auftretenden Konstanten an; man überzeugt sich aber durch eine numerische Verfolgung des Beweises leicht, daß q jedenfalls größer als 2 ausfällt.

In den folgenden Zeilen werde ich zeigen, daß man durch eine Verschärfung der dem Landauschen Beweis zugrunde liegenden Ideen zu einem Beweis des oben erwähnten Tschebyschefschen Satzes gelangen kann, der — wie mir scheint — an Einfachkeit nicht hinter dem Ramanujanschen Beweis steht. Griechische Buchstaben sollen im Folgenden durchwegs positive, lateinische Buchstaben natürliche Zahlen bezeichnen; die Bezeichnung p ist für Primzahlen vorbehalten.

1. Der Binomialkoeffizient

$$\binom{2a}{a} = \frac{(2a)!}{(a!)^2}$$

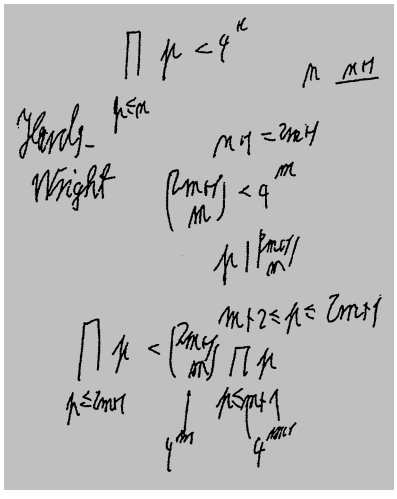
[1]) Srr. Ramanujan, A Proof of Bertrand's Postulate, *Journal of the Indian Mathematical Society*. 11 (1919). S. 181—182 — *Collected Papers of* Srinivasa Ramanujan (Cambridge, 1927), S. 208—209.

есть последовательность простых чисел, в которой каждое последующее меньше удвоенного предыдущего. Поэтому каждый интервал $\{y : n < y \leq 2n\}$, где $n \leq 4000$, содержит одно из этих 14 простых чисел.

(2) Далее докажем, что

$$\prod_{p \leq x} p \;\leq\; 4^{x-1} \quad \text{для всех вещественных } x \geq 2, \tag{1}$$

запись $\prod_{p \leq x} p$ здесь и в дальнейшем означает, что произведение берется по всем *простым* числам $p \leq x$.



Приведенное ниже доказательство этого факта использует индукцию по числу простых. Оно не содержится в оригинальной статье Эрдёша, но также принадлежит ему (см. рисунок на полях) и является истинным Доказательством из Книги.

Вначале заметим, что если q — наибольшее простое, не превосходящее x, то

$$\prod_{p \leq x} p \;=\; \prod_{p \leq q} p \qquad \text{и} \qquad 4^{q-1} \;\leq\; 4^{x-1}.$$

Таким образом, (1) достаточно проверить в случае $x = q$, где q — простое число.

Если $q = 2$, мы имеем «$2 \leq 4$», так что база индукции обоснована, и мы далее будем рассматривать нечетные числа $q = 2m + 1$. Разобьем произведение на две части и убедимся в том, что

$$\prod_{p \leq 2m+1} p \;=\; \prod_{p \leq m+1} p \cdot \prod_{m+1 < p \leq 2m+1} p \;\leq\; 4^m \binom{2m+1}{m} \;\leq\; 4^m 2^{2m} \;=\; 4^{2m}.$$

Действительно, неравенство

$$\prod_{p \leq m+1} p \;\leq\; 4^m$$

справедливо в силу предположения индукции. Неравенство

$$\prod_{m+1 < p \leq 2m+1} p \;\leq\; \binom{2m+1}{m}$$

вытекает из того, что

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$$

есть целое число и что все входящие в произведение простые числа являются делителями числителя $(2m+1)!$, но ни одно из них не является делителем знаменателя $m!(m+1)!$ Наконец, неравенство

$$\binom{2m+1}{m} \;\leq\; 2^{2m}$$

вытекает из того, что

$$\binom{2m+1}{m} \quad \text{и} \quad \binom{2m+1}{m+1}$$

суть два (равных!) слагаемых в сумме

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}.$$

Итак, соотношение (1) доказано по индукции.

(3) Согласно приведенной на полях теореме Лежандра, разложение биномиального коэффициента $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ на простые множители содержит p ровно

$$\sum_{k\geq 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right)$$

раз. Каждое слагаемое в этой сумме не превосходит 1, так как оно является целым числом и

$$\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor < \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1\right) = 2.$$

Более того, слагаемые, для которых $p^k > 2n$, равны нулю. Поэтому разложение $\binom{2n}{n}$ содержит простой множитель p

$$\sum_{k\geq 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right) \leq \max\{r : p^r \leq 2n\}$$

раз. Следовательно, наибольшая степень числа p, которая делит $\binom{2n}{n}$, не превосходит $2n$. В частности, каждое простое $p > \sqrt{2n}$ появляется в разложении $\binom{2n}{n}$ не более одного раза.

Кроме того (и это, согласно Эрдёшу, является ключом к его доказательству), простые p, удовлетворяющие условию $\frac{2}{3}n < p \leq n$, вообще не являются делителями числа $\binom{2n}{n}$. Действительно, из условия $3p > 2n$ следует (для $n \geq 3$, и, следовательно, для $p \geq 3$), что из кратных простого p в качестве множителей в числитель дроби $\frac{(2n)!}{n!n!}$ могут входить только p и $2p$, в то время как в знаменателе мы уже имеем два множителя, равных p.

(4) Теперь перейдем к оценке $\binom{2n}{n}$. Для $n \geq 3$, используя неравенство со с. 20 в качестве нижней оценки, получаем

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq \prod_{p\leq\sqrt{2n}} 2n \cdot \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \cdot \prod_{n<p\leq 2n} p,$$

и, так как существует не более $\sqrt{2n}$ простых чисел $p \leq \sqrt{2n}$, отсюда для $n \geq 3$ находим:

$$4^n \leq (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \cdot \prod_{n<p\leq 2n} p. \qquad (2)$$

(5) Предположим теперь, что простых чисел в промежутке $n < p \leq 2n$ не содержится, так что второе произведение в (2) равно 1. Подставляя (1) в (2), находим

$$4^n \leq (2n)^{1+\sqrt{2n}}\, 4^{\frac{2}{3}n},$$

Теорема Лежандра

Простое число p входит в разложение числа $n!$ на простые множители ровно

$$\sum_{k\geq 1}\left\lfloor\frac{n}{p^k}\right\rfloor$$

раз.

■ **Доказательство.** В произведении $n! = 1\cdot 2\cdot 3\cdot\ldots\cdot n$ ровно $\lfloor\frac{n}{p}\rfloor$ сомножителей делятся на p, что дает $\lfloor\frac{n}{p}\rfloor$ простых множителей p в разложении $n!$ Далее, $\lfloor\frac{n}{p^2}\rfloor$ чисел среди $1,\ldots,n$ делятся на p^2, что дает еще $\lfloor\frac{n}{p^2}\rfloor$ простых множителей p в разложении $n!$, и т. д. □

Примеры
$\binom{26}{13} = 2^3\cdot 5^2\cdot 7\cdot 17\cdot 19\cdot 23$
$\binom{28}{14} = 2^3\cdot 3^3\cdot 5^2\cdot 17\cdot 19\cdot 23$
$\binom{30}{15} = 2^4\cdot 3^2\cdot 5\cdot 17\cdot 19\cdot 23\cdot 29$
показывают, что «очень малые» простые множители $p < \sqrt{2n}$ могут входить в разложение $\binom{2n}{n}$ с большими степенями, «малые» простые из промежутка $\sqrt{2n} < p \leq \frac{2}{3}n$ могут быть только в первой степени, а простые множители из лакуны $\frac{2}{3}n < p \leq n$ вообще отстутствуют.

или

$$4^{\frac{1}{3}n} \leq (2n)^{1+\sqrt{2n}}, \tag{3}$$

что для достаточно больших n неверно! В самом деле, так как $a+1 < 2^a$ для всех $a \geq 2$, то

$$2n = \left(\sqrt[6]{2n}\right)^6 < \left(\left\lfloor \sqrt[6]{2n} \right\rfloor + 1\right)^6 < 2^{6\left\lfloor \sqrt[6]{2n} \right\rfloor} \leq 2^{6\sqrt[6]{2n}}. \tag{4}$$

При $n \geq 50$ (когда $18 < 2\sqrt{2n}$) из (3) и (4) вытекает, что

$$2^{2n} \leq (2n)^{3\left(1+\sqrt{2n}\right)} < \left(2^{6\sqrt[6]{2n}}\right)^{3\left(1+\sqrt{2n}\right)} =$$

$$= 2^{\sqrt[6]{2n}\left(18+18\sqrt{2n}\right)} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}.$$

Поэтому $(2n)^{1/3} < 20$, вследствие чего $n < 4000$. Значит, для любого $n \geq 4000$ существует такое простое число p, что $n < p < 2n$. □

Из приведенной выше оценки (2) тем же самым способом можно извлечь большее: для $n \geq 4000$

$$\prod_{n<p\leq 2n} p \geq 2^{\frac{1}{30}n},$$

и поэтому в промежутке между n и $2n$ имеется не менее

$$\log_{2n}\left(2^{\frac{1}{30}n}\right) = \frac{1}{30}\,\frac{n}{\log_2 n + 1}$$

простых чисел. Это не слишком грубая оценка: «истинное» число простых чисел в указанном промежутке равно приблизительно $n/\log n$, что следует из «закона распределения простых чисел», согласно которому

$$\lim_{n\to\infty} \frac{\#\{p \leq n : p \text{ простое}\}}{n/\log n}$$

существует и равен 1 (запись $\#A$ обозначает число элементов множества A). Этот замечательный результат был впервые доказан Адамаром и де ла Валле-Пуссеном в 1896 году[1]. Селберг и Эрдёш в 1948 году нашли элементарное доказательство без использования комплексного анализа, но длинное и сложное.

В законе распределения простых чисел последнее слово, однако, еще не сказано. Например, доказательство гипотезы Римана (см. с. 50), одной из главных нерешенных проблем математики, может привести к существенному уточнению оценок в теореме о простых числах. Можно надеяться также на значительное усиление постулата Бертрана. Например, следующее предложение еще не доказано:

[1] Важным шагом на пути к теореме Адамара и Валле-Пуссена были работы П.Л.Чебышёва ([5*], [6*], см. также [7*]), из которых следовало, что

$$0,921 < \frac{\#\{p \leq n : p \text{ простое }\}}{n/\log n} < 1,106$$

при достаточно больших n. Отметим также один из последних результатов (см. [8*]):

$$\#\{p \leq n : p \text{ простое}\} < \frac{n}{\log n - 1 - \sqrt{\log n}} \text{ при } n \geq 6,$$

$$\#\{p \leq n : p \text{ простое}\} > \frac{n}{\log n - 1 + \sqrt{\log n}} \text{ при } n \geq 59.$$

— *Прим. ред.*

В промежутке между n^2 и $(n+1)^2$ всегда найдется простое число.

Дополнительную информацию можно найти в [3, с. 19] и [4, с. 248, 257].

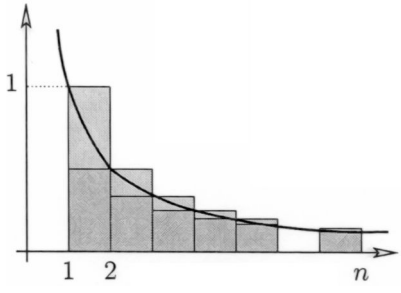
Приложение: Некоторые оценки

Оценки с помощью интегралов

Существует очень простой, но эффективный метод оценивания сумм с помощью интегралов, использованный на с. 11. Для оценивания *гармонических чисел*

$$H_n = \sum_{k=1}^{n} \frac{1}{k}$$

рассмотрим приведенные на полях графики функций $\frac{1}{t}$, $\frac{1}{\lceil t \rceil}$ и $\frac{1}{1+\lfloor t \rfloor}$.



Неравенство

$$H_n - 1 = \sum_{k=2}^{n} \frac{1}{k} < \int_1^n \frac{1}{t}\,dt = \log n$$

доказывается сравнением области под графиком функции $f(t) = \frac{1}{t}$ $(1 \le t \le n)$ с областью, состоящей из темных заштрихованных прямоугольников, а неравенство

$$H_n - \frac{1}{n} = \sum_{k=1}^{n-1} \frac{1}{k} > \int_1^n \frac{1}{t}\,dt = \log n$$

— сравнением с областью, состоящей из больших прямоугольников и включающей светлые заштрихованные части. Объединяя эти оценки, получаем

$$\log n + \frac{1}{n} < H_n < \log n + 1.$$

В частности, $\lim\limits_{n\to\infty} H_n = \infty$, и порядок роста чисел H_n описывается соотношением $\lim\limits_{n\to\infty} \frac{H_n}{\log n} = 1$. Известны также (см. [2]) значительно лучшие оценки, например

$$H_n = \log n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} + O\left(\frac{1}{n^6}\right),$$

где $\gamma \approx 0,5772$ — «константа Эйлера».

Здесь запись $O\left(\frac{1}{n^6}\right)$ обозначает функцию $g(n)$ такую, что $|g(n)| \le c\frac{1}{n^6}$, где c — некоторая константа.

Оценки факториалов — формула Стирлинга

Тот же самый метод, примененный к сумме

$$\log(n!) = \log 2 + \log 3 + \ldots + \log n = \sum_{k=2}^{n} \log k,$$

приводит к оценкам

$$\log((n-1)!) < \int_1^n \log t\,dt < \log(n!),$$

и интеграл легко вычисляется:

$$\int_1^n \log t\,dt \;=\; \Big[t\log t - t\Big]_1^n \;=\; n\log n - n + 1.$$

Отсюда мы получаем как оценку снизу для $n!$

$$n! \;>\; e^{n\log n - n + 1} \;=\; e\Big(\frac{n}{e}\Big)^n,$$

так и оценку сверху

$$n! \;=\; n\,(n-1)! \;<\; ne^{n\log n - n + 1} \;=\; en\Big(\frac{n}{e}\Big)^n.$$

Здесь выражение $f(n) \sim g(n)$ означает, что $\lim\limits_{n\to\infty} \dfrac{f(n)}{g(n)} = 1$.

Чтобы найти асимптотику $n!$, требуется более тонкий анализ, который приводит к *формуле Стирлинга*

$$n! \;\sim\; \sqrt{2\pi n}\Big(\frac{n}{e}\Big)^n.$$

И снова существуют ее уточненные варианты, например:

$$n! \;=\; \sqrt{2\pi n}\Big(\frac{n}{e}\Big)^n\left(1 + \frac{1}{12n} + \frac{1}{288n^2} - \frac{139}{5140n^3} + O\left(\frac{1}{n^4}\right)\right).$$

Оценки биномиальных коэффициентов

Как известно, непосредственно из определения биномиальных коэффициентов $\binom{n}{k}$ как числа k-подмножеств n-множества следует, что последовательность $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$:

- суммируется и $\sum\limits_{k=0}^{n} \binom{n}{k} = 2^n$,
- симметрична: $\binom{n}{k} = \binom{n}{n-k}$.

```
                1
              1   1
            1   2   1
          1   3   3   1
        1   4   6   4   1
      1   5  10  10   5   1
    1   6  15  20  15   6   1
  1   7  21  35  35  21   7   1
```

Треугольник Паскаля

Из функционального уравнения $\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$ легко найти, что для каждого n биномиальные коэффициенты $\binom{n}{k}$ образуют последовательность, которая симметрична и *унимодальна*: ее элементы возрастают при приближении к середине, так что средние биномиальные коэффициенты являются наибольшими:

$$1 = \tbinom{n}{0} < \tbinom{n}{1} < \ldots < \tbinom{n}{\lfloor n/2\rfloor} = \tbinom{n}{\lceil n/2\rceil} > \ldots > \tbinom{n}{n-1} > \tbinom{n}{n} = 1.$$

Из асимптотических формул для факториалов, упомянутых выше, можно получить очень точные оценки для биномиальных коэффициентов. Однако в этой книге нам понадобятся лишь довольно грубые и простые оценки, например, $\binom{n}{k} \le 2^n$ для всех k. С другой стороны, для $n \ge 2$ имеем

$$\binom{n}{\lfloor n/2\rfloor} \;\ge\; \frac{2^n}{n},$$

причем равенство выполняется только при $n = 2$. В частности, для $n \ge 1$

$$\binom{2n}{n} \;\ge\; \frac{4^n}{2n}.$$

Действительно, так как центральный биномиальный коэффициент $\binom{n}{\lfloor n/2 \rfloor}$ является максимальным в последовательности

$$\binom{n}{0} + \binom{n}{n}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1},$$

сумма всех n элементов которой равна 2^n, то он больше среднего значения элементов этой последовательности, равного $\frac{2^n}{n}$.

Наконец, отметим еще одну верхнюю оценку для биномиальных коэффициентов:

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!} \leq \frac{n^k}{k!} \leq \frac{n^k}{2^{k-1}};$$

она довольно хороша для «малых» биномиальных коэффициентов из хвостов образуемой ими последовательности, если n велико по сравнению с k.

Литература

[1] Erdős P. *Beweis eines Satzes von Tschebyschef.* Acta Sci. Math. (Szeged), **5** (1930–32), 194–198.

[2] Graham R. L., Knuth D. E., Patashnik O. *Concrete Mathematics. A Foundation for Computer Science.* Addison-Wesley, Reading MA, 1989. [Есть русский перевод: Грэхем Р., Кнут Д., Паташник О. *Конкретная математика. Основание информатики.* М., Мир, 1998.]

[3] Hardy G. H., Wright E. M. *An Introduction to the Theory of Numbers,* 5th edition. Oxford University Press, 1979.

[4] Ribenboim P. *The New Book of Prime Number Records.* Springer-Verlag, New York, 1989.

[5*] Chebyshev P. L. *Mémoire sur les nombres premies.* Mémoires des savants étrangers de l'Acad. Imp. Sci. de St.-Pétersbourg, 1850, t.VII; J. de math. pures et appl., I série, 1852, t.XVII; русский перевод: *О простых числах.* В сб. Чебышёв П. Л. *Избранные математические труды,* М.-Л., ГИТТЛ, 1946, с.53–72; *Избранные труды,* изд-во АН СССР, М., 1955, с.33–54.

[6*] Chebyshev P. *Sur la fonction qui détermine la totalité des nombers premiers inférieurs à une limite donnée.* — Приложение III к Теории сравнений, С.-Петербург, 1849; Mémoires des savants étrangers de l'Acad. Imp. Sci. de St.-Pétersbourg, 1848, t.VI; J. de math. pures et appl., I série, 1852, t.XVII; русский перевод: *Об определении числа простых чисел, не превосходящих данной величины.* В сб. Чебышёв П. Л. *Избранные математические труды,* М.-Л., ГИТТЛ, 1946, с.29–52, *Избранные труды,* изд-во АН СССР, 1955, с.9–32.

[7*] Делоне Б. Н. *Петербургская школа теории чисел.* М.-Л, изд-во АН СССР, 1947.

[8*] Panaitopol L. *Inequalities concerning the function $\pi(x)$: Applications.* Acta Arithmetica, 2000, v.XCIV, № 4, 373–381.