Распределение простых чисел

Райгородский Андрей Михайлович

24 февраля 2020 г. — 26 февраля 2020 г.

«Анекдот из жизни: семинар в МГУ. Семинарист — выдающийся специалист по теории чисел, по диофантовым уравнениям. Приходит кто-то, говорит, что доцент и послушает семинар. Этот доцент выдержал весь семинар, на семинаре рассказывали распределение простых чисел. После семинара не удержался, спрашивает, занимался ли кто-то тут диофантовыми уравнениями. Специалист говорит, что нет, потому что понял, что ферматист. Тогда доцент спрашивает про простые числа. И говорит: вот, придумал два простых числа и два других простых числа, перемножил и получил одно и то же!» — Райгородский

Определение 1. $\pi(x)$ — количество простых чисел, не больших x.

Определение 2. $\nu(x)$ — количество различных простых чисел в разложении x на простые множители. Например, $\nu(2^4 \cdot 5^{11} \cdot 7^{12345}) = 3$.

Мы хотим как-то оценить $\pi(x)$ и $\nu(x)$. Для этого нам понадобятся следующие функции:

Определение 3. $\vartheta(x)$ — сумма по всем $p \le x$ их натуральных логарифмов.

Определение 4. $\psi(x)$ — сумма по всем $p \le x$ их натуральных логарифмов с коэффициентами $\alpha_p = \lfloor \log_p x \rfloor$.

«Когда я начинал заниматься наукой, я выбирал обозначение для случайной величины — $M\eta$ или $E\eta$. Выбирал из соображений патриотизма — M от слова Матожидание, а E — от слова Expectation. Когда я привык, я узнал, что M от слова Mid Value...» — Райгородский

Определение 5. Математическое ожидание $\mathbb{E}X$ случайной величины X — сумма $X(G)P(G)$. В частности, если все события равновероятны, $\mathbb{E}X = \frac{\sum X(G)}{|\Omega|}$.

Утверждение. $\mathbb{E}[c_1X_1 + c_2X_2] = c_1\mathbb{E}X_1 + c_2\mathbb{E}X_2$.

Пример. Пусть X — количество треугольников в графе. Тогда считать $\mathbb{E}X$ по определению очень сложно (получается $\sum\limits_i iP(X = i)$ и очевидно, например, как считать графы без треугольников). Рассмотрим такие $\binom{n}{3}$ случайных величин:

$$Y_{ijk}(V, E) = \begin{cases} 1, (i,j) \in E, (j,k) \in E, (k,i) \in E \\ 0, \text{ иначе} \end{cases}$$

Тогда, с одной стороны, $\mathbb{E}Y_{ijk} = \frac{1}{8}$, с другой стороны, $\mathbb{E}X = \mathbb{E}[\sum\limits_{i,j,k} Y_{ijk}] = \sum\limits_{i,j,k} \mathbb{E}Y_{ijk} = \binom{n}{3} \cdot \frac{1}{8}$.

Определение 6. Дисперсия случайной величины — $\mathbb{D}X = \mathbb{E}[(X - \mathbb{E}X)^2]$.

Лемма 1. $\mathbb{D}X = \mathbb{E}[X^2] - \mathbb{E}^2X$.

Доказательство. Раскроем скобки и получим нужное равенство. ■

Теорема 2 (Марков). Пусть $X \ge 0$ и $a > 0$. Тогда $P(X > a) \le \frac{\mathbb{E}X}{a}$.

Доказательство.

$$\mathbb{E}X = \sum_i y_iP(X = y_i) = \sum_{y_i > a} y_iP(X = y_i) + \sum_{y_j \le a} y_jP(X = y_j) \ge \sum_{y_i > a} y_iP(X = y_i) > aP(x > a). \blacksquare$$

Теорема 3 (Чебышёв). Пусть $a > 0$. Тогда $P(|X - \mathbb{E}X| > a) \le \frac{\mathbb{D}X}{a^2}$.

Доказательство. Пусть $Y = (X - \mathbb{E}X)^2$. Применим 2 для Y и a^2. Получим $P((X - \mathbb{E}X)^2 > a^2) \le \frac{\mathbb{D}X}{a^2}$, откуда следует утверждение задачи. ■

Обозначим $\limsup \frac{\vartheta(x)}{x} = \lambda_1, \limsup \frac{\psi(x)}{x} = \lambda_2, \limsup \frac{\pi(x)\ln x}{x} = \lambda_3$.

Лемма 4. $\lambda_1 = \lambda_2 = \lambda_3$.

Доказательство. Очевидно, что $\vartheta(x) \le \psi(x) \le \pi(x)\ln x$. Значит, $\lambda_1 \le \lambda_2 \le \lambda_3$.

Докажем, что $\lambda_3 \le \lambda_1$. Зафиксируем любое $\alpha \in [0,1)$. Тогда

$$\vartheta(x) = \sum_{p\le x} \ln p \ge \sum_{x^\alpha < p \le x} \ln p \ge \sum_{x^\alpha < p \le x} \ln(x^\alpha) = \alpha \ln x \sum_{x^\alpha < p \le x} 1 = \alpha \ln x(\pi(x) - \pi(x^\alpha) \ge \alpha \ln x(\pi(x) - x^\alpha).$$

Поделим обе части на x. Получим

$$\frac{\vartheta(x)}{x} \ge \frac{\alpha \ln x}{x}(\pi(x) - x^\alpha) = \alpha\left(\frac{\pi(x)\ln x}{x} - \frac{\ln x}{x^{1-\alpha}}\right).$$

Заметим, что $\ln x < x^\beta$ при любом $\beta > 0$ начиная с какого-то момента. Подставим $\beta = 1 - \alpha$. Это значит, что второе слагаемое стремится к 0 вне зависимости от α, то есть $\lambda_1 \ge \alpha\lambda_3$ при любом $\alpha < 1$. Перейдём к пределу $\alpha \to 1$, получим искомый результат. ■

Аналогично можно доказать, что $\mu_1 = \liminf \frac{\vartheta(x)}{x} = \mu_2 = \liminf \frac{\psi(x)}{x} = \mu_3 = \liminf \frac{\pi(x)\ln x}{x}$.

Теорема 5 (Чебышёв). Существуют a, b такие, что $0 < a < b < \infty$ и для любого x выполняется $\frac{ax}{\ln x} \le \pi(x) \le \frac{bx}{\ln x}$.

Доказательство. Рассмотрим $f(n) = \binom{2n}{n}$. Заметим, что оно лежит между $\frac{2^{2n}}{2n+1}$ и 2^{2n}. Кроме того,

$$f(n) \ge \prod_{n<p<2n} p \implies 2n\ln 2 > \ln f(n) \ge \sum_{n<p<2n} \ln p = \vartheta(2n) - \vartheta(n).$$

Подставим $n = 1, 2, 4, \ldots, 2^{k-1}$ и просуммируем. Получим $\vartheta(2^k) < 2^k \cdot 2\ln 2$. Кроме того, т.к. $\vartheta(x)$ не убывает, то $\vartheta(x) < 4x\ln 2$. Тогда по 4 получаем $\pi(x)\ln x < 4x\ln 2$ в пределе. Таким образом, подходит $b = 4\ln 2$.

Теперь докажем, что подходит $a = \ln 2$. Заметим, что

$$\binom{2n}{n} = \prod_{p\le 2n} p^{\sum_j \left\lfloor \frac{2n}{p^j}\right\rfloor - 2\left\lfloor \frac{n}{p^j}\right\rfloor} \le \prod_{p\le 2n} p^{\sum_j 1} = \prod_{p\le 2n} p^{\left\lfloor \frac{\ln 2n}{\ln p}\right\rfloor}.$$

Прологарифмируем обе части неравенства:

$$2n\ln 2 - \ln(2n+1) \le \ln\binom{2n}{n} \le \sum_{p\le 2n} \ln p \left\lfloor \frac{\ln 2n}{\ln p}\right\rfloor = \psi(2n).$$

Т.к. второе слагаемое левой части растёт медленно, получаем $\mu_2 \ge \ln 2$. Тогда $\mu_3 \ge \ln 2$. ■

Теорема 6. Пусть $n \in [x]$. Тогда почти наверное почти верно $\nu(n) = c\ln\ln x$. Более точно,

$$P\left[|\nu(x) - \ln\ln n| \ge \omega(n)\sqrt{\ln\ln n}\right] \to 0, n \to \infty, x \in \{1, \ldots, n\},$$

где $\omega(n)$ — любая наперёд заданная функция, которая стремится к ∞.

Доказательство. Если мы хотим вывести это неравенство из 3, мы хотим доказать, что $\mathbb{E}[\nu(n)] = \mathbb{D}[\nu(n)] = \ln\ln n$.

Для подсчёта $\mathbb{E}\nu$ введём величины $\nu_p(x) = 1$ для $x \equiv 0 \mod p$ и $\nu_p(x)$ иначе. Тогда

$$\mathbb{E}\nu = \mathbb{E}\left[\sum_{p\le n} \nu_p\right] = \sum_{p\le n} \mathbb{E}\nu_p = \sum_{p\le n} \frac{\left\lfloor \frac{n}{p}\right\rfloor}{n}.$$

Лемма 7. $p_m \sim m \ln m$.

Доказательство. Пусть мы знаем, что $\pi(x) \sim \frac{x}{\ln x}$. Допустим, это не так. Пусть, например, $p_m > x = cm \ln m$ для $c > 1$ с какого-то момента. Тогда $m > \pi(x) \sim \frac{x}{\ln x} = \frac{cm \ln m}{\ln(cm \ln m)} \sim cm > m$ — противоречие. ■

' **Лемма 8.** $SP_n = \frac{1}{p_1} + \frac{1}{p_2} + \ldots + \frac{1}{p_n} \sim \ln \ln n$.

Доказательство. $SP_n \sim \int_1^n \frac{1}{x \ln x} dx$. С другой стороны, $(\ln \ln x)' = \frac{1}{\ln x} \cdot \frac{1}{x} = \frac{1}{x \ln x}$. ■

Продолжим разбираться с $\mathbb{E}\nu$:

$$\mathbb{E}\nu = \sum_{p \le n} \frac{\left\lfloor \frac{n}{p} \right\rfloor}{n} = \sum_{p \le n} \left(\frac{1}{p} + O\left(\frac{1}{n}\right) \right) = \ln \ln n + O(1) + O\left(\frac{1}{\ln n}\right) = \ln \ln n + O(1).$$

Осталось оценить $\mathbb{D}\nu$:

$$\mathbb{D}\nu \sim \mathbb{E}\nu^2 - \ln \ln^2 n = \mathbb{E}\left[\sum \nu_p^2 + \sum_{(p,q) \le n} \nu_p \nu_q \right] - \ln \ln^2 n \sim \ln \ln n - \ln \ln^2 n + \sum_{(p,q) \le n} \frac{\left\lfloor \frac{n}{pq} \right\rfloor}{n}.$$

На этом месте у нас возникают трудности, потому что эта сумма слишком большая. Но можно вместо ν рассматривать ν' — количество простых делителей n, каждый из которых меньше $\sqrt[5]{n}$. Эти числа различаются максимум на 4, поэтому асимптотически это не важно, но эта сумма сильно уменьшилась и стала пропорциональна $\frac{5n^{0.4}}{n \ln^2 n}$. Значит, и дисперсия, и матожидание стали порядка $\Theta(\ln \ln n)$, что и требовалось получить. ■