Труды по дискретной математике
Том 11, с. 43–50
М.: ФИЗМАТЛИТ, 2008

ВЕРОЯТНОСТНЫЕ ПРЕДСТАВЛЕНИЯ МЕР, СВЯЗАННЫХ С РАЗЛОЖЕНИЯМИ НА МНОЖИТЕЛИ

А. М. ЗУБКОВ

Для разработки современных теоретико-числовых алгоритмов (в частности, алгоритмов факторизации и дискретного логарифмирования по простому модулю) и оценки их эффективности большое значение имеют теоремы и формулы, описывающие распределение простых чисел и натуральных чисел без больших простых делителей, так называемых гладких (smooth) чисел. Ряд нетривиальных и весьма точных асимптотических формул получен методами аналитической теории чисел. В настоящей работе показано, что меры, порожденные подмножествами натуральных чисел, представимых в виде произведений чисел из заданных множеств, можно представить в виде смесей вероятностных мер, порожденных произведениями независимых целочисленных случайных величин. Обсуждаются возможности использования таких представлений.

§ 1. ВВЕДЕНИЕ. КРАТКАЯ СВОДКА РЕЗУЛЬТАТОВ ИЗ ТЕОРИИ ЧИСЕЛ

Пусть, как обычно, $\pi(y)$ обозначает число простых чисел, не превосходящих y. Согласно теоремам о распределении простых чисел (см., например, [1, 12]) для некоторого $c > 0$ при $y \to \infty$ справедливы соотношения

$$\pi(y) = (1 + o(1))\frac{y}{\ln y}, \quad \pi(y) = \int\limits_2^y \frac{dt}{\ln t} + O\left(ye^{-c\sqrt{\ln y}}\right).$$

В [11] доказаны следующие неравенства:

$$\pi(y) < \frac{y}{\ln y - 1 - \sqrt{\ln y}} \quad \text{при } y \geqslant 6,$$

$$\pi(y) > \frac{y}{\ln y - 1 + \sqrt{\ln y}} \quad \text{при } y \geqslant 59.$$

Пусть, далее, $D(n)$ обозначает максимальный простой делитель n, а функция

$$\Psi(x, y) = |\{n \in \{1, \ldots, x\} \colon D(n) \leqslant y\}|$$

© А. М. Зубков, 2008

— количество натуральных чисел, не превосходящих x и не имеющих простых делителей, бóльших y. Первая асимптотическая формула для $\Psi(x,y)$ была получена Дикманом в 1930 году (см. [7]): при любом фиксированном $u>0$

$$\lim_{y\to\infty}\Psi(y^u,y)\,y^{-u}=\rho(u),$$

где функция $\rho(u)$ определяется как единственное непрерывное решение дифференциально-разностного уравнения

$$u\rho'(u)=-\rho(u-1),\quad u>1,$$

с начальными условиями $\rho(u)=1$, $0\leqslant u\leqslant 1$. Позднее этот результат Дикмана уточнялся и обобщался в работах ряда математиков. В частности, в [10] доказано, что

$$\Psi(x,y)=x\rho(u)\left(1+O\left(\frac{\ln(1+u)}{\ln y}\right)\right),\quad u=\frac{\ln x}{\ln y}=\ln_y x,$$

где для любого $\varepsilon>0$ константа в $O(\cdot)$ равномерна в области

$$y\geqslant 2,\quad 1\leqslant u\leqslant\exp\left\{(\ln y)^{3/5-\varepsilon}\right\}$$

и при $u\geqslant 1$

$$\rho(u)=\exp\left\{-u\left(\ln u+\ln\ln(u+2)-1+O\left(\frac{\ln\ln(u+2)}{\ln(u+2)}\right)\right)\right\},$$

а в [12] — что

$$\ln\Psi(x,y)=Z\left\{1+O\left(\frac{1}{\ln y}+\frac{1}{\ln\ln x}\right)\right\},$$

где

$$Z=Z(x,y)=\frac{\ln x}{\ln y}\ln\left(1+\frac{y}{\ln x}\right)+\frac{y}{\ln y}\ln\left(1+\frac{\ln x}{y}\right)$$

и константа в $O(\cdot)$ допускает равномерную оценку в области $x\geqslant y\geqslant 2$.

Получены также некоторые результаты о количестве гладких чисел в интервалах небольшой длины. В частности, Харман [9] показал, что для каждого $\varepsilon>0$ отрезок $[x,x+\sqrt{x}\,]$ при достаточно больших x содержит порядка $\sqrt{x}$ чисел, все простые делители которых меньше $x^{1/(4\sqrt{e}+\varepsilon)}$. Фридландер и Лагариас [8] доказали существование такой абсолютной константы c, что при $\beta>1-\alpha-c\alpha(1-\alpha)^3$ отрезок $[x,x+x^\beta]$ содержит порядка x^β чисел, все простые делители которых меньше x^α. В недавней работе [6] показано, что для любого $\varepsilon>0$ существует такое $c=c(\varepsilon)$, что для всех достаточно больших x отрезок $[x,x+c\sqrt{x}\,]$ содержит не менее $\sqrt{x}\,/(\ln x)^{\ln 4+o(1)}$ чисел, все делители которых не больше $x^{47/(190\sqrt{e})+\varepsilon}$.

В [5] доказано, что если $0<\alpha<\beta<1$, а $\Psi(x,x^\beta,x^\alpha)$ — количество натуральных чисел, не превосходящих x и таких, что все их простые делители

не больше x^β, а число простых делителей, бóльших x^α, не превышает 1, то при $x \to \infty$

$$\Psi(x, x^\beta, x^\alpha) = x\rho\left(\frac{1}{\alpha}\right) + x\int\limits_\alpha^\beta \frac{1}{\lambda}\rho\left(\frac{1-\lambda}{\alpha}\right)\,d\lambda + O\left(\frac{|\ln\alpha|}{\alpha(1-\beta)}\,\frac{x}{\ln x}\right).$$

Там же описаны методы практического вычисления функции $\Psi(x, x^\beta, x^\alpha)$ и приведены таблицы ее значений.

Эти результаты получены тонкими аналитическими методами, существенно использующими свойства функции $\pi(n)$. В [4] обсуждаются возможности использования представления распределения совокупности компонент случайных комбинаторных структур в виде условного распределения совокупности независимых целочисленных случайных величин при условии, наложенном на значения их суммы. Такие представления, впервые использованные В. Ф. Колчиным [2] при изучении схемы размещения частиц по ячейкам, оказались удобными при доказательстве предельных теорем для случайных подстановок, разбиений, отображений, полиномов и т. п. Однако применение этого подхода к изучению свойств разложения простых чисел на множители, как показано в [4], сталкивается с существенными трудностями.

В настоящей работе показано, что меру, которая сосредоточена на множестве целых чисел, представимых в виде произведений ограниченного количества натуральных чисел из заданного конечного множества W, и приписывает всем элементам этого множества одно и то же значение, можно представить в виде смеси (линейной комбинации) вероятностных распределений произведений степеней независимых случайных величин, равномерно распределенных на W. Коэффициенты этой линейной комбинации выписываются в явном виде, и основной вклад в это представление дает относительно малая часть всей суммы, что в принципе можно использовать, например, для оценки значений функций типа $\Psi(x, y)$, построенных не только по произведениям всех простых чисел, но и по произведениям чисел из заданных конечных множеств.

§ 2. ОПИСАНИЕ ПРЕДСТАВЛЕНИЯ

Пусть $\mathbf{N}_+ = \{1, 2, \ldots\}$ — множество натуральных чисел, $W = \{q_1, \ldots, q_w\}$ — совокупность взаимно простых натуральных чисел, $2 \leqslant q_1 < q_2 < \ldots < q_w$. Пусть W^a — множество всех натуральных чисел, представимых в виде произведений ровно a чисел из W (такие представления определяются однозначно в силу взаимной простоты элементов W, поэтому множества W^a попарно не пересекаются) и $W^* = \cup_{a\geqslant 1} W^a$. Введем целочисленную меру ν_W на $\mathbf{N}_+$, полагая $\nu_W(\{n\}) = I(n \in W^*)$. Тогда, например,

$\Psi(x,y) = \nu_W(\{1,\dots,x\})$, $x \in \mathbf{N}_+$, если W — совокупность всех простых чисел, не превосходящих y.

Определим вектор-функцию $\alpha = (\alpha_1,\dots,\alpha_w)\colon \mathbf{N}_+ \to \mathbf{N}_+^w$ как набор показателей в разложении n в произведение чисел из W:

$$\alpha(n) = \begin{cases} (\alpha_1,\dots,\alpha_w), & \text{если } n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_w^{\alpha_w}, \\ (0,\dots,0), & \text{если } n \notin W^*; \end{cases}$$

положим $|\alpha(n)| = \alpha_1 + \ldots + \alpha_w$.

Введем на $\mathbf{N}_+$ меры $\nu_{W,a}$, $a \in \mathbf{N}_+$, равенствами

$$\nu_{W,a}(n) = I(n \in W^*,\ |\alpha(n)| = a),$$

тогда

$$\nu_W = \sum_{a \geqslant 1} \nu_{W,a}; \tag{1}$$

в сумме (1) для $\nu_W(n)$ при $n \leqslant x$ отличны от 0 только слагаемые с $a \leqslant \ln_{q_1} x$.

Основным результатом настоящей работы является следующее утверждение.

Теорема. *Пусть ζ_{ij} — независимые случайные величины, имеющие равномерное распределение на конечном множестве $W = \{q_1 < q_2 < \ldots \ldots < q_w\} \in \{2,3,\ldots\}$, состоящем из взаимно простых чисел. Тогда при любых натуральных r и n*

$$\sum_{a=1}^{r} \nu_{W,a}(n) = \sum_{\substack{m_1,m_2,\dots,m_r \geqslant 0:\\ m_1+2m_2+\ldots+rm_r \leqslant r}} \mathbf{P}\left\{\prod_{\beta=1}^{r}\prod_{j=1}^{m_\beta} \zeta_{\beta,j}^{\beta} = n\right\} \prod_{\beta=1}^{r} \frac{w^{m_\beta}}{\beta^{m_\beta} m_\beta!}.$$

В частности, количество натуральных чисел, не превосходящих x и представимых в виде произведения чисел из W, допускает представление

$$\left|\sum_{a=1}^{[\ln_{q_1} x]} \nu_{W,a}(\{2,\dots,[x]\})\right| =$$

$$= \sum_{\substack{m_1,m_2,\dots,m_{[\ln_{q_1} x]} \geqslant 0:\\ m_1+2m_2+\ldots+[\ln_{q_1} x]m_{[\ln_{q_1} x]} \leqslant [\ln_{q_1} x]}} \mathbf{P}\left\{\sum_{\beta=1}^{r} \beta \sum_{j=1}^{m_\beta} \ln \zeta_{\beta,j} \leqslant \ln x\right\} \prod_{\beta=1}^{r} \frac{w^{m_\beta}}{\beta^{m_\beta} m_\beta!}.$$

Доказательство. Мере $\nu_{W,a}$ можно поставить в соответствие полную симметрическую функцию

$$h_a = h_a(x_1,\dots,x_w) = \sum_{1 \leqslant i_1 \leqslant i_2 \leqslant \ldots \leqslant i_a \leqslant w} x_{i_1} x_{i_2} \dots x_{i_a} = \sum_{n:|\alpha(n)|=a} \prod_{i=1}^{w} x_i^{\alpha_i(n)},$$

поскольку в силу единственности разложения на простые множители и взаимной простоты элементов множества W множество значений одночленов $x_{i_1}x_{i_2}\dots x_{i_a}$ в этой сумме при $x_j = q_j$, $j = 1,\dots,w$, совпадает с множеством $\{n \in \mathbf{N}_+ \colon |\alpha(n)| = a\}$. Отметим, что по той же причине

$$h_a(e^{z\ln q_1},\dots,e^{z\ln q_w}) = \sum_{n\colon |\alpha(n)|=a} e^{z\ln n}.$$

Согласно (1) мере ν_W соответствует формальный симметрический ряд

$$h = \sum_{a\geqslant 1} h_a = \sum_{a\geqslant 1}\ \sum_{1\leqslant i_1\leqslant i_2\leqslant\dots\leqslant i_a\leqslant w} x_{i_1}x_{i_2}\dots x_{i_a}. \tag{2}$$

В монографии [3] устанавливаются связи между функциями h_a и степенными суммами (симметрическими функциями от тех же аргументов)

$$s_\beta = s_\beta(x_1,\dots,x_w) = \sum_{i=1}^{w} x_i^\beta, \quad \beta \in \mathbf{N}_+.$$

Для полноты изложения проведем вывод соответствующих формул. Производящая функция для многочленов $h_a = h_a(x_1,\dots,x_w)$ ($h_0 = 1$) имеет вид

$$H(t) = \sum_{a\geqslant 0} h_a t^a = \prod_{i=1}^{w}\sum_{k=0}^{\infty} x_i^k t^k = \prod_{i=1}^{w}\frac{1}{1-x_i t}.$$

С другой стороны, производящей функцией многочленов s_β является

$$S(t) = \sum_{\beta=1}^{\infty} s_\beta t^{\beta-1} = \sum_{i=1}^{w}\sum_{\beta=1}^{\infty} x_i^\beta t^{\beta-1} = \sum_{i=1}^{w}\frac{x_i}{1-x_i t} = \sum_{i=1}^{w}\frac{d}{dt}\ln\frac{1}{1-x_i t}.$$

Поэтому

$$S(t) = \frac{d}{dt}\ln\prod_{i=1}^{w}\frac{1}{1-x_i t} = \frac{d}{dt}\ln H(t) = \frac{H'(t)}{H(t)}, \tag{3}$$

т. е. $H'(t) = S(t)H(t)$. Из явного вида решения этого уравнения относительно функции $H(t)$ (с начальным условием $H(0) = 1$) можно получить выражение h_a через s_β:

$$H(t) = \sum_{a\geqslant 0} h_a t^a = \exp\left\{\int_0^t S(u)\,du\right\} = \exp\left\{\sum_{\beta=1}^{\infty}\frac{1}{\beta}s_\beta t^\beta\right\} =$$

$$= \prod_{\beta=1}^{\infty}\exp\left\{\frac{1}{\beta}s_\beta t^\beta\right\} = \prod_{\beta=1}^{\infty}\sum_{m_\beta=0}^{\infty}\frac{(s_\beta t^\beta)^{m_\beta}}{\beta^{m_\beta}m_\beta!} = \sum_{m_1,m_2,\dots=0}^{\infty} t^{\sum_{\beta\geqslant 1}\beta m_\beta}\prod_{\beta\geqslant 1}\frac{s_\beta^{m_\beta}}{\beta^{m_\beta}m_\beta!}.$$

Таким образом, при любом $a \geqslant 1$

$$h_a = \sum_{\substack{m_1,m_2,\ldots,m_a \geqslant 0:\\ m_1+2m_2+\ldots+am_a=a}} \prod_{\beta=1}^{a} \frac{1}{\beta^{m_\beta} m_\beta!} s_\beta^{m_\beta}$$

и при любом $r \in \mathbf{N}_+$

$$\sum_{a=1}^{r} h_a = \sum_{a=1}^{r} \sum_{\substack{m_1,m_2,\ldots,m_a \geqslant 0:\\ m_1+2m_2+\ldots+am_a=a}} \prod_{\beta=1}^{a} \frac{1}{\beta^{m_\beta} m_\beta!} s_\beta^{m_\beta} =$$

$$= \sum_{\substack{m_1,m_2,\ldots,m_r \geqslant 0:\\ m_1+2m_2+\ldots+rm_r \leqslant r}} \prod_{\beta=1}^{r} \frac{1}{\beta^{m_\beta} m_\beta!} s_\beta^{m_\beta}. \quad (4)$$

Из этой формулы и отмеченного ранее соответствия между мерой ν_W и функцией h следует, что мера ν_W является линейной комбинацией (с положительными коэффициентами $\prod_{\beta=1}^{r}(\beta^{m_\beta} m_\beta!)^{-1}$) мер

$$\sigma_{m_1,\ldots,m_a}, \quad m_1, m_2, \ldots, m_a \geqslant 0, \ a \leqslant r,$$

соответствующих симметрическим многочленам

$$S_{m_1,\ldots,m_a}(x_1,\ldots,x_w) = \prod_{\beta=1}^{a} s_\beta^{m_\beta} = \prod_{\beta=1}^{a} \left(\sum_{i=1}^{w} x_i^\beta \right)^{m_\beta}, \quad (5)$$

а именно: каждый одночлен $\prod_{\beta=1}^{a} \prod_{j=1}^{m_\beta} x_{i(\beta,j)}^\beta$ в разложении произведения (5) дает вклад в меру $\sigma_{m_1,\ldots,m_a}$ в виде единичной массы в точке (натуральном числе) $\prod_{\beta=1}^{a} \prod_{j=1}^{m_\beta} p_{i(\beta,j)}^\beta$. В отличие от мер ν_W и $\nu_{W,a}$, атомы мер $\sigma_{m_1,\ldots,m_a}$ могут иметь разные ненулевые массы (они соответствуют количествам представлений натурального числа в виде произведений чисел из W с учетом порядка сомножителей).

Меры $\sigma_{m_1,\ldots,m_a}$ допускают простую вероятностную интерпретацию: если $m = m_1 + m_2 + \ldots + m_a$, а случайные величины $\zeta_{i,j}$ $(i, j \in \mathbf{N}_+)$ независимы и

$$\mathbf{P}\{\zeta_{i,j} = q_k\} = \frac{1}{w}, \quad k \in \{1,\ldots,w\}, \ i,j \geqslant 1,$$

то

$$\frac{1}{w^m} S_{m_1,\ldots,m_a}(e^{z\ln q_1},\ldots,e^{z\ln q_w}) =$$

$$= \prod_{\beta=1}^{a} \left(\sum_{i=1}^{w} \frac{1}{w} e^{z\beta \ln q_i} \right)^{m_\beta} = \mathbf{E} \exp\left\{ z \sum_{\beta=1}^{a} \sum_{j=1}^{m_\beta} \beta \ln \zeta_{\beta,j} \right\},$$

т. е. мера $\sigma_{m_1,\ldots,m_a}$ (с точностью до нормирующего множителя w^m) соответствует распределению произведения $\prod_{\beta=1}^{a}\prod_{j=1}^{m_\beta}\zeta_{\beta,j}^{\beta}$ независимых случайных величин.

Отсюда и из (1), (2), (4) следует, что при любом $n \in \mathbf{N}_+$ меру $\sum_{a=1}^{r}\nu_{W,a}$ можно представить в виде смеси мер, порожденных произведениями степеней независимых случайных величин, равномерно распределенных на W:

$$\sum_{a=1}^{r}\nu_{W,a}(n) = \sum_{\substack{m_1,m_2,\ldots,m_r\geqslant 0:\\ m_1+2m_2+\ldots+rm_r\leqslant r}} \sigma_{m_1,\ldots,m_r}(n)\prod_{\beta=1}^{r}\frac{1}{\beta^{m_\beta}m_\beta!} =$$

$$= \sum_{\substack{m_1,m_2,\ldots,m_r\geqslant 0:\\ m_1+2m_2+\ldots+rm_r\leqslant r}} \mathbf{P}\left\{\prod_{\beta=1}^{r}\prod_{j=1}^{m_\beta}\zeta_{\beta,j}^{\beta} = n\right\}\prod_{\beta=1}^{r}\frac{w^{m_\beta}}{\beta^{m_\beta}m_\beta!}.$$

Теорема доказана.

Заметим еще, что из (3) следуют также соотношения

$$ah_a = \sum_{\beta=1}^{a} s_\beta h_{a-\beta}, \quad a \in \mathbf{N}_+, \tag{6}$$

или

$$\begin{pmatrix} -1 & 0 & 0 & \ldots & 0 & 0 \\ s_1 & -2 & 0 & \ldots & 0 & 0 \\ s_2 & s_1 & -3 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ s_{a-1} & s_{a-2} & s_{a-3} & \ldots & s_1 & -a \end{pmatrix}\begin{pmatrix} h_1 \\ h_2 \\ h_3 \\ \vdots \\ h_a \end{pmatrix} = \begin{pmatrix} -s_1 \\ -s_2 \\ -s_3 \\ \vdots \\ -s_a \end{pmatrix}.$$

Решение этой системы линейных уравнений по правилу Крамера дает другое выражение для функций h_a через s_β:

$$h_a = \frac{1}{a!}\begin{vmatrix} -1 & 0 & 0 & \ldots & 0 & -s_1 \\ s_1 & -2 & 0 & \ldots & 0 & -s_2 \\ s_2 & s_1 & -3 & \ldots & 0 & -s_3 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ s_{a-2} & s_{a-3} & s_{a-4} & \ldots & -a+1 & -s_{a-1} \\ s_{a-1} & s_{a-2} & s_{a-3} & \ldots & s_1 & -s_a \end{vmatrix} =$$

$$= \frac{(-1)^a}{a!} \begin{vmatrix} s_1 & -1 & 0 & \dots & 0 & 0 \\ s_2 & s_1 & -2 & \dots & 0 & 0 \\ s_3 & s_2 & s_1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_{a-1} & s_{a-2} & s_{a-3} & \dots & s_1 & -a+1 \\ s_a & s_{a-1} & s_{a-2} & \dots & s_2 & s_1 \end{vmatrix}. \tag{7}$$

СПИСОК ЛИТЕРАТУРЫ

1. *Карацуба А.А.* Основы аналитической теории чисел. — М.: Наука, ГРФМЛ, 1983.
2. *Колчин В.Ф.* Один класс предельных теорем для условных распределений. — Лит. матем. сб., 1968, т. 8, № 1, с. 53–63.
3. *Макдональд И.* Симметрические функции и многочлены Холла. — М.: Мир, 1985.
4. *Arratia R., Barbour A.D., Tavaré S.* Random combinatorial structures and prime factorizations. — Notices of Amer. Math. Soc., 1997, v. 44, № 8, p. 903–910.
5. *Bach E., Peralta R.* Asymptotic semismoothness probabilities. — Math. Comput., 1996, v. 65, p. 1701–1715.
6. *Croot E.* Smooth numbers in short intervals. — http://www.math.gatech.edu/~ecroot/smooth6.pdf
7. *Dickman K.* On the frequency of numbers containing prime factors of a certain relative magnitude. — Ark. Mat. Astr. Fys., 1930, v. 22, p. 1–14.
8. *Friedlander J., Lagarias J.* On the distribution in short intervals of integers having no large prime factor. — J. Number Theory, 1987, v. 25, p. 249–273.
9. *Harman G.* Integers without large prime factors in short intervals and arithmetic progressions. — Acta Arith., 1999, v. 91, p. 279–289.
10. *Hildebrand A.* On the number of positive integers $\leqslant x$ and free of prime factors $> y$. — J. Number Theory, 1986, v. 22, p. 265–290.
11. *Panaitopol L.* Inequalities concerning the function $\pi(x)$: Applications. — Acta Arithmetica, 2000, v. XCIV, № 4, p. 373–381.
12. *Tenenbaum G.* Introduction à la théorie analytique et probabiliste des nombres. — Publ. Inst. Elie Cartan., 1990, v. 13. Univ. Nancy 1.