Применение вероятностных методов в теории чисел

Довольно удачно и строго о связях теории вероятностей и теории чисел написано, например, в книге М. Каца “Статистическая независимость в теории вероятностей, анализе и теории чисел”. М.: ИЛ, 1963. В качестве, руководства по теории чисел рекомендуется ознакомиться с книгой И.М. Виноградова “Основы теории чисел”, выдержавшей большое число изданий.

Задача (Г. Вейль). Рассмотрим последовательность $\{a_k\}_{k\in\mathbb{N}}$, где a_k - первая цифра в десятичной записи числа 2^k. Положим $I_m(a_k)=\begin{cases}1, & a_k=m\\ 0, & a_k\neq m\end{cases}$ $(m=1,2,...,9)$. Существует ли $\lim\limits_{n\to\infty}\dfrac{1}{n}\sum\limits_{k=1}^{n}I_m(a_k)$? Если существует, то найдите его.

Указание. Рассмотрим вероятностное пространство $X=(\Omega,\Xi,P)$, где $\Omega=[0,1)$, Ξ - σ-алгебра борелевских множеств[1] на $[0,1)$, а P - равномерная мера на Ξ, т.е. $P([a,b))=b-a$. Рассмотрим с.в.

$$x(\omega)=\begin{cases}1, & \omega\in[\log_{10}m,\log_{10}(m+1))\\ 0, & \omega\in[0,\log_{10}m)\cup[\log_{10}(m+1),1)\end{cases}.$$

Рассмотрим случайный процесс (в дискретном времени)

$X_k(\omega)=x(T^k\omega)$, где $T:[0,1)\to[0,1)$ определяется по формуле[2] $T\omega=(\omega+\log_{10}2)\mod 1$.

Покажите, что случайный процесс X_k - стационарный в узком смысле. В предположении, что этот процесс эргодичен по математическому ожиданию[3] найдите искомый предел[4].

---

[1] Т.е. Ξ - минимальная σ-алгебра, содержащая всевозможные открытые множества $\Omega=[0,1)$.

[2] Важно заметить, что преобразование T сохраняет меру, т.е. $\forall\ A\in\Xi\to P(T^{-1}A)=P(A)$. Собственно, и в более общей ситуации, известная из курса случайных процессов эргодическая теорема схожим образом переносится на динамические системы, которые задаются фазовым пространством Ω и динамикой $T:\ \Omega\to\Omega$. Согласно теореме Крылова – Боголюбова (см. Я.Г. Синай, Введение в эргодическую теорию, М.: ФАЗИС, 1996, лекция 2), если Ω - компакт, то всегда найдется как минимум одна инвариантная относительно T мера на Ξ. Если построенной по такой динамической системе случайный процесс окажется эргодическим, то доля времени пребывания динамической системы в заданной области просто равняется мере (той самой инвариантной и эргодической) этой области. Ввиду вышесказанного интересно заметить, что установление эргодичности является трудной задачей. До сих пор строго не обоснована “эргодическая гипотеза Лоренца” для идеального газа в сосуде (см. В.В. Козлов, Тепловое равновесие по Гиббсу и Пуанкаре, Москва – Ижевск, РХД, 2002, Р. Минлос, Введение в математическую статистическую физику, М.: МЦНМО, 2002).

[3] См. А.Н. Ширяев, Вероятность-2, М.: МЦНМО, 2004, глава 5, § 2.

[4] Стоит обратить внимание, что в эргодической теореме фигурирует сходимость либо в L_2, либо в L_1, либо п.н.. А в данной задаче требуется (для доказательства существования предела и его вычисления), сходимость

***Задача (Гаусса – Гильдена – Вимана – Кузьмина)*[5].** Каждое число из промежутка $\Omega=[0,1)$ может быть разложено в цепную дробь (вообще говоря, бесконечную). Цепные дроби играют важную роль, например, в различных вычислениях (поскольку позволяют строить в определенном смысле наилучшие приближения иррациональных чисел рациональными), в теории динамических систем (КАМ теории). Для рациональных чисел такие дроби конечны, для квадратичных иррациональностей – периодические (см. пример ниже, в котором период равен 1):[6]

$$\frac{\sqrt{5}-1}{2}=\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ldots}}}=\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ldots}}}.$$

Покажите, что, не смотря на приведенный выше пример, для почти всех (в равномерной мере) точек $\omega\in[0,1)$

$$\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}I_m\left(a_k(\omega)\right)=\frac{1}{\ln 2}\ln\left(1+\frac{1}{m(m+2)}\right).$$

Указание. Покажите, что преобразование $T:\ [0,1)\to[0,1)$

$$T\omega=\begin{cases}\left\{\dfrac{1}{\omega}\right\}, & \omega\in(0,1)\\ 0, & \omega=0\end{cases},$$

где $\{5.8\}=0.8$ - дробна часть числа, сохраняет меру Гаусса

$$\forall\ A\in\Xi\to P(A)=\frac{1}{\ln 2}\int_A\frac{dx}{1+x}.$$

Далее рассуждайте аналогично предыдущей задаче (эргодичность возникшего случайного процесса можно не доказывать).

Задача (КАМ теория). Число α из отрезка $[0,1]$ назовем нормально приближаемым рациональными числами, если найдутся c, $\varepsilon>0$ такие, что при любом натуральном q

---

поточечная. Оказывается, для данной задачи из сходимости в L_2 легко следует сходимость п.н., откуда (в свою очередь) следует поточечная (подробности см. Я.Г. Синай, Введение в эргодическую теорию, М.: ФАЗИС, 1996, лекция 3 и И.П. Корнфельд, Я.Г. Синай, С.В. Фомин, Эргодическая теория, М.: Наука, 1980).

[5] См. В.И. Арнольд, Цепные дроби, М.: МЦНМО, 2001.

[6] Чтобы проверить выписанное соотношение достаточно заметить, что $\frac{\sqrt{5}-1}{2}$ - является корнем уравнения $x=\frac{1}{1+x}$ (причем, из принципа сжимающих отображений следует, что последовательность $x_{n+1}=\frac{1}{1+x_n}$, $x_0=1$ сходится именно к этому корню).

$$\min_{p\in\mathbb{Z}}\left|\alpha-\frac{p}{q}\right|\geq\frac{c}{q^{2+\varepsilon}}.$$

Используя лемму Бореля - Кантелли докажите, что множество нормально приближаемых чисел на отрезка $[0,1]$ имеет Лебегову меру 1.

Указание. Зафиксируем c, $\varepsilon>0$ и рассмотрим множество

$$A_q=\left\{\alpha\in[0,1]\,\middle|\,\min_{p\in\mathbb{Z}}\left|\alpha-\frac{p}{q}\right|<\frac{c}{q^{2+\varepsilon}}\right\}.$$

Покажите, что $\mu(A_q)\leq\frac{2c}{q^{1+\varepsilon}}$. Таким образом, ряд $\sum_q\mu(A_q)$ сходится. В силу леммы Бореля-Кантелли отсюда следует нужное утверждение.

Заметим, что эта задача пришла из теории динамических систем на двумерном торе. Подобного же рода задачи возникают и в КАМ теории.

В связи с полученным результатом, будет интересно заметить, что существует такая бесконечная последовательность q_k и соответствующая ей последовательность p_k, что

$$\left|\alpha-\frac{p_k}{q_k}\right|<\frac{1}{\sqrt{5}}\frac{1}{{q_k}^2}.$$

В теории цепных дробей показывается, что последовательность $\frac{p_k}{q_k}$ - будет подпоследовательностью последовательности подходящих дробей для числа α. Заметим также, что константу $\frac{1}{\sqrt{5}}$ в неравенстве уменьшить нельзя.

Синай Я.Г. Основы эргодической теории. М.: ФАЗИС, 1996.

Задача (вероятностное доказательство формулы Эйлера). Пусть X – целочисленная случайная величина с распределением

$$P(X=n)=\frac{1}{\varsigma(s)n^s},\ \text{где}\ \varsigma(s)=\sum_{n\in\mathbb{N}}n^{-s},\quad s>1.$$

Пусть $1<p_1<p_2<p_3<\ldots$ - простые числа, и пусть A_k - событие = {X делится на p_k}.

А) Найдите $P\{A_k\}$ и покажите, что события $A_1,A_2,\ldots$независимы.

Б) Покажите, что

$$\prod_{k=1}^{\infty}(1-{p_k}^{-s})=\frac{1}{\varsigma(s)}\ (\textit{формула Эйлера}).$$

Кельберт М.Я., Сухов Ю.М. Вероятность и статистика в примерах и задачах. Т. 1. Основные понятия теории вероятностей и математической статистики. М.: МЦНМО, 2007.

Довольно часто вероятностные соображения (например, независимость) используются в теории чисел не совсем строго, но зато весьма часто они позволяют угадать правильный ответ. Поясним сказанное, пожалуй, наиболее популярным примером из уже цитированной книги известного американского математика прошлого века Марка Каца.

Пусть A – некоторое множество положительных целых чисел. Обозначим через $A(n)$ количество тех его элементов, которые содержатся среди первых n чисел натурального ряда. Если существует предел $\lim_{n\to\infty} A(n)/n = P(A)$, то он называется плотностью A. К сожалению, вероятностная мера $P(A)$ не является вполне аддитивной (счетно аддитивной).

Рассмотрим целые числа, делящиеся на простое число p. Плотность множества таких чисел, очевидно, равна $1/p$. Возьмем теперь множество целых чисел, которые делятся одновременно на p и q (q - другое простое число). Делимость на p и q эквивалентна делимости на pq, и, следовательно, плотность нового множества равна $1/pq$.Так как $1/pq = (1/p)\cdot(1/q)$, то мы можем истолковать это так: “события”, заключающиеся в делимости на p и q, независимы. Это, конечно, выполняется для любого количества простых чисел.

Поставим теперь задачу посчитать “вероятность” несократимости дроби (фиксируется знаменатель дроби n, а затем случайно, с равной вероятностью $1/n$ выбирается любое число от 1 до n в качестве числителя, и подсчитывается доля случаев, в которых полученная дробь оказывалась несократимой) в следующем (Чезаровском) смысле (здесь и далее индекс p может пробегать только простые числа):

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\frac{\#\{k<n:\ Н.О.Д.(n,k)=1\}}{n}=\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\frac{\varphi(n)}{n}=\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\prod_{p}\left(1-\frac{\rho_p(n)}{p}\right),\ \text{где}$$

$\varphi(n)$ - функция Эйлера, $\rho_p(n)=\begin{cases}1, & n \text{ делится на } p\\ 0, & \text{иначе}\end{cases}$.

Легко проверить, что предела в обычном смысле не существует.

Но согласно введенному выше определению плотности:

$$M\left\{\prod_{p\le p_k}\left(1-\frac{\rho_p(n)}{p}\right)\right\}=\prod_{p\le p_k}M\left\{\left(1-\frac{\rho_p(n)}{p}\right)\right\}=\prod_{p\le p_k}\left(1-\frac{1}{p^2}\right).$$

С учетом этого хочется написать следующее:

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\frac{\varphi(n)}{n}=M\left\{\frac{\varphi(n)}{n}\right\}=M\left\{\prod_{p}\left(1-\frac{\rho_p(n)}{p}\right)\right\}=\prod_{p}\left(1-\frac{1}{p^2}\right)=\frac{1}{\varsigma(2)}=\frac{6}{\pi^2}.$$

Будь введенная вероятностная мера, по которой считается это математическое ожидание, счетно аддитивной, то можно было бы поставить точку, получив ответ. Однако, это не так. Хотя ответ мы и получили правильный, но приведенное выше рассуждение не может считаться доказательством. Впрочем, часто вероятностные рассуждения удается пополнить, используя их в качестве основы. Так в разобранном нами примере все сводится к обоснованию равенства

$$M\left\{\prod_{p}\left(1-\frac{\rho_p(n)}{p}\right)\right\}=\prod_{p}M\left\{\left(1-\frac{\rho_p(n)}{p}\right)\right\}.$$

Известный российский математик Владимир Игоревич Арнольд последние десять лет жизни активно развивал описанное направление, которое он называл “Экспериментальной математикой” (помимо популярных книжек и статей, осталось и несколько видеолекций на эту тему http://www.mathnet.ru/php/presentation.phtml?option_lang=rus, с выступлениями на семинаре МИАНа, в летней школе Современная математика и на мехмате). Получая схожим образом “ответы”, их далее можно проверять, ставя численные эксперименты. При современных возможностях вычислительных машин, можно отслеживать логарифмические функции в асимптотике (т.е. проверять гипотезы с логарифмами), но не с повторными логарифмами, которые также как и в случайных процессах встречаются в теории чисел. Таким образом, у В.И. получалось довольно много теорем (десятки, а возможно, даже сотни). Часть теорем, конечно, была известна ранее (см., например, книгу А.А. Карацубы “Основы аналитической теория чисел”. М.: Наука, 1975), но удавалось получать и новые формулировки.

Следующий пример, взятый из другой книги М. Каца “Вероятность и смежные вопросы в физике”. М.: Мир, 1965, демонстрирует, что отмеченным выше способом можно получить и неверный результат.

Пример (из журнала Nature, 1940). Из изложенного выше следует, что число целых чисел, не превосходящих N и не делящихся ни на одно из простых чисел p_1, p_2, …, p_k, равно приблизительно $N\prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right)$. Рассмотрим теперь число целых чисел, не превосходящих N и не делящихся ни на одно из простых чисел, меньших $\sqrt{N}$. Такими числами могут быть только простые числа, лежащие между $\sqrt{N}$ и N, число которых $\pi(N)-\pi\left(\sqrt{N}\right)\sim N\prod_{p_j<\sqrt{N}}\left(1-\frac{1}{p_j}\right)$. Но из теории чисел известно, что $\pi(N)\sim N/\ln N$ и $\prod_{p_j<\sqrt{N}}\left(1-\frac{1}{p_j}\right)\sim \exp(-\gamma)/\ln\sqrt{N}=2\exp(-\gamma)/\ln N$, где γ - константа Эйлера. Следовательно, $2\exp(-\gamma)=1$. Пришли к неверному соотношению!

Интересно в этой связи отметить также вероятностный способ получения правильной асимптотической формулы $\pi(N)\sim N/\ln N$ для числа простых чисел, не превосходящих N, приведенный в книге Р. Куранта и Г. Роббинса “Что такое математика”. М.: МЦНМО, 2007.

Задача (вероятностный метод в теории чисел; Харди – Рамануджан – Туран – Эрдёш - Кац, 1920, 1934, 1940)*.** Пусть $\nu(n)$ обозначает количество простых чисел p, делящих n. Тогда для любого λ

$$\lim_{n\to\infty}\frac{1}{n}\left|\left\{k:1\le k\le n,\nu(k)\ge \ln\ln n+\lambda\sqrt{\ln\ln n}\right\}\right|=\frac{1}{\sqrt{2\pi}}\int_{\lambda}^{\infty}e^{-t^2/2}dt\,.$$

Алон Н., Спенсер Дж. Вероятностный метод. М.: Бином, 2007.

Задача (предельные меры; А.М. Вершик и др., 1977). В качестве множества элементарных исходов рассматривается группа всевозможных подстановок (перестановок) S_n (симметрическая группа), $n\gg 1$. В этой группе $n!$ элементов. Припишем каждой подстановке одинаковую вероятность $1/n!$.

А)* Покажите, что математическое ожидание числа циклов есть $\approx \ln n$.

Б)** В каком смысле нормированные длины циклов случайной подстановки убывают со скоростью геометрической прогрессии со знаменателем e^{-1}.

В)** Положим $\rho_n(a) = \left|\left\{g \in S_n : n_{\max}(g) \le an\right\}\right| / n!$, где $n_{\max}(g)$ - длина максимально цикла в подстановке g. Покажите, что $\rho_n(a)$ удовлетворяет *уравнению Дикмана – Гончарова* (40-ые годы XX века):

$$\rho_n(a) = \int_0^a \rho_n\left(\frac{a}{1-t}\right) dt .$$

Г)*** Покажите, что начиная с некоторого большого числа N 99% натуральных чисел n, больших, чем N обладают свойством: $n^{0.99} < p_1 \cdot \ldots \cdot p_{11}$. Иначе говоря, у основной части (99%) натуральных чисел основная часть (99%) числа есть произведение наибольших простых делителей. Число 11 возникло из-за того, что мы выбрали 99% и 99%.

Указание. Решение задач всех пунктов сводится (весьма технически нетривиально!) к задаче о "ломании палки". Отрезок $[0,1]$ делится ("ломается") случайно с равномерной вероятностью. Левый отрезок фиксируем, а правый ломается аналогичным образом и т.д..

Вершик А.М., Шмидт А.А. Предельные меры, возникающие в асимптотической теории симметрических групп // ТВП, Т. 22. № 1. 1977.С. 72-88; Т. 23. № 1. 1978. С. 42-54.

Вершик А.М. Асимптотическое распределение разложений натуральных чисел на простые делители // ДАН, 1986. Т. 289, № 2. С. 269–272.

http://www.mathnet.ru/PresentFiles/231/v231.pdf

http://www.mathnet.ru/php/presentation.phtml?option_lang=rus&presentid=231

Durrett R. Probability: Theory and examples. 2010

http://uqu.edu.sa/files2/tiny_mce/plugins/filemanager/files/4281670/probability/mathematics/mathematics1/math6/math8/Durrett%20R.%20Probability%20Theory.pdf

В заключение заметим, что применение вероятностных соображений в теории чисел продолжает привлекать ведущих математиков и по сей день (см. выступление Я.Г. Синая):
http://erb-files.narod.ru/#GLOBUS