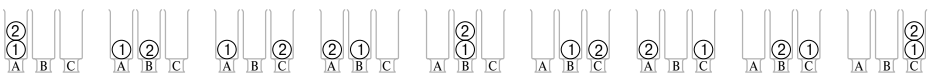
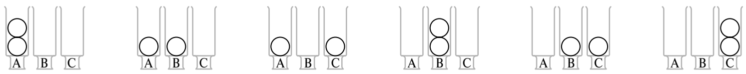
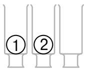
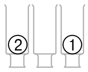
7.2.1.4 Генерация всех разбиений

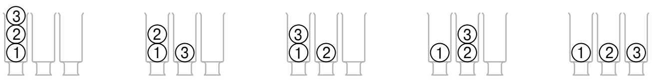
Великолепная книга Ричарда Стенли (Richard Stanley) *Перечислительная комбинаторика* (*Enumerative Combinatorics*, 1986) начинается с рассмотрения "двенадцатизадачия" — массива размером $2 \times 2 \times 3$ фундаментальных комбинаторных задач, часто возникающих на практике (табл. 1). Все 12 задач Стенли можно описать в терминах распределения заданного количества шаров по заданному количеству урн. Например, имеется девять способов поместить два шара в три урны, если и шары и урны помечены.



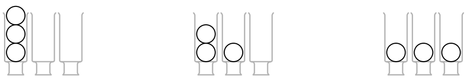
(Порядок шаров *внутри* урны игнорируется.) Но если шары не помечены, то некоторые из размещений неразличимы, так что возможны только шесть различных способов размещения.

 (1)

Если урны не помечены, то размещения наподобие  и , по сути, одинаковы, следовательно, различимы только два из исходных девяти размещений. Если же у нас имеется три помеченных шара, то вот все различные способы их размещения в трех непомеченных урнах.

 (2)

И наконец, если ни шары, ни урны не помечены, то приведенные пять способов размещения сводятся только к трем.

 (3)

Двенадцатизадачие рассматривает все возможные распределения для помеченных и непомеченных урн и шаров, а также необязательное требование, чтобы в каждой урне содержалось не менее (не более) одного шара.

В предыдущих разделах данной главы мы рассмотрели n-кортежи, перестановки, сочетания и композиции; две из двенадцати записей табл. 1 тривиальны — размещение n вещей по m приемным карманам. Таким образом, мы можем завершить наше изучение классической комбинаторной математики рассмотрением оставшихся пяти записей таблицы, которые включают *разбиения* (partitions).

Начнем с того, что слово "разбиение" в математике имеет множество значений. Оно возникает всякий раз, когда выполняется разделение некоторого объекта на подобъекты.

— Джордж Эндрюс (George Andrews), Теория разбиений (The Theory of Partitions) (1976)

Таблица 1. Двенадцатизадачие

Шары в урнах	Без ограничений	$\leqslant 1$	$\geqslant 1$
n помеченных шаров, m помеченных урн	n-кортежи из m вещей	n-перестановки m вещей	разбиения $\{1,\ldots,n\}$ на m упорядоченных частей
n непомеченных шаров, m помеченных урн	n-мультисочетания из m вещей	n-сочетания m вещей	композиции n из m частей
n помеченных шаров, m непомеченных урн	разбиения $\{1,\ldots,n\}$ на $\leqslant m$ частей	n вещей в m приемных карманов	разбиения $\{1,\ldots,n\}$ на m частей
n непомеченных шаров, m непомеченных урн	разбиения n на $\leqslant m$ частей	n вещей в m приемных карманов	разбиения n на m частей

Одно и то же имя имеют две достаточно разные концепции: *разбиение множества* — это способы его разделения на непересекающиеся подмножества; таким образом, (2) представляет собой иллюстрацию пяти разбиений $\{1,2,3\}$, а именно:

$$\{1,2,3\}\,, \quad \{1,2\}\{3\}\,, \quad \{1,3\}\{2\}\,, \quad \{1\}\{2,3\}\,, \quad \{1\}\{2\}\{3\}\,. \tag{4}$$

Разбиения целого числа представляют собой способы записи его в виде суммы положительных целых чисел, независимо от их порядка. Так, в (3) показаны три разбиения числа 3, а именно

$$3, \quad 2+1, \quad 1+1+1. \tag{5}$$

Мы будем следовать общей практике и называть разбиения целых чисел просто “разбиениями”, не указывая их объекта; другой вид мы будем называть “разбиениями множеств”, чтобы ясно указывать различия между этими видами разбиений. Оба вида разбиений важны, так что мы изучим их по очереди.

Генерация всех разбиений целых чисел. Разбиение числа n формально можно определить как последовательность неотрицательных целых чисел $a_1 \geqslant a_2 \geqslant \cdots$, такую, что $n = a_1 + a_2 + \cdots$; например, одно из разбиений $7 - a_1 = a_2 = 3$, $a_3 = 1$ и $a_4 = a_5 = \cdots = 0$. Количество ненулевых членов называется количеством *частей*, а нулевые члены обычно опускаются. Таким образом, мы записываем $7 = 3+3+1$, или просто 331, чтобы сэкономить место, если контекст очевиден.

Простейший (и один из быстрейших) способ сгенерировать все разбиения — посетить их в обратном лексикографическом порядке, начиная с ‘n’ и заканчивая ’11…1’. Например, разбиения 8 в указанном порядке представляют собой

$$\begin{gathered}8, 71, 62, 611, 53, 521, 5111, 44, 431, 422, 4211, 41111, 332, 3311,\\ 3221, 32111, 311111, 2222, 22211, 221111, 2111111, 11111111.\end{gathered} \tag{6}$$

Если разбиение состоит не из одних единиц, оно завершается некоторым числом $(x+1)$, где $x \geqslant 1$, за которым следует ноль или несколько единиц. Следовательно, очередное наименьшее разбиение в лексикографическом порядке получается путем замены суффикса $(x+1)\,1\ldots1$ на $x\ldots xr$ для некоторого соответствующего остатка $r \leqslant x$. Процесс достаточно эффективен, если отслеживать наибольший индекс q, такой, что $a_q \neq 1$, как предложено Д.К.С. Маккеем (J.K.S. McKay) [*CACM*, **13** (1970), 52], и заполнять массив единицами, как предложили А. Зогби (A. Zoghbi) и И. Стойменович (I. Stojmenovic) [*International Journal of Computer Math.*, **70** (1998), 319–332].

Алгоритм P (Разбиения в обратном лексикографическом порядке). Этот алгоритм генерирует все разбиения $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_m \geqslant 1$ с $a_1 + a_2 + \cdots + a_m = n$ и $1 \leqslant m \leqslant n$ при $n \geqslant 1$. Значение a_0 также устанавливается равным 0.

P1. [Инициализация.] Установить $a_m \leftarrow 1$ для $n \geqslant m > 1$. Затем установить $m \leftarrow 1$ и $a_0 \leftarrow 0$.

P2. [Сохранить заключительную часть.] Установить $a_m \leftarrow n$ и $q \leftarrow m - [n = 1]$.

P3. [Посещение.] Посетить разбиение $a_1 a_2 \ldots a_m$. Затем, если $a_q \neq 2$, перейти к шагу P5.

P4. [Замена 2 на 1+1.] Установить $a_q \leftarrow 1$, $q \leftarrow q - 1$, $m \leftarrow m + 1$ и вернуться к шагу P3. (В этот момент $a_k = 1$ для $q < k \leqslant n$.)

P5. [Уменьшение a_q.] Завершить работу, если $q = 0$. В противном случае установить $x \leftarrow a_q - 1$, $a_q \leftarrow x$, $n \leftarrow m - q + 1$ и $m \leftarrow q + 1$.

P6. [Копирование x при необходимости.] Если $n \leqslant x$, вернуться к шагу P2. В противном случае установить $a_m \leftarrow x$, $m \leftarrow m + 1$, $n \leftarrow n - x$ и повторить данный шаг. ▮

Обратите внимание, что переход от одного разбиения к следующему выполняется особенно просто, если имеется двойка; шаг P4 просто изменяет крайнюю справа двойку на единицу и добавляет единицу справа. Эта приятная ситуация, к счастью, представляет собой наиболее распространенный случай. Например, при $n = 100$ около 79% всех разбиений содержат 2.

Если мы хотим генерировать все разбиения числа n на фиксированное количество частей, к нашим услугам другой простой алгоритм. Приведенный далее метод, разработанный в диссертации К.Ф. Гинденбурга (C.F. Hindenburg) в 18-м веке [*Infinitinomii Dignitatum Exponentis Indeterminati* (Göttingen, 1779), 73–91], посещает все разбиения в *солексном* (colex) порядке, т.е. лексикографическом порядке “отраженных” последовательностей $a_m \ldots a_2 a_1$.

Алгоритм H (Разбиение на m частей). Этот алгоритм генерирует все целые m-кортежи $a_1 \ldots a_m$, такие, что $a_1 \geqslant \ldots \geqslant a_m \geqslant 1$ и $a_1 + \cdots + a_m = n$, в предположении, что $n \geqslant m \geqslant 2$.

H1. [Инициализация.] Установить $a_1 \leftarrow n{-}m{+}1$ и $a_j \leftarrow 1$ для $1 < j \leqslant m$. Установить также $a_{m+1} \leftarrow -1$.

H2. [Посещение.] Посетить разбиение $a_1 \ldots a_m$. Затем, если $a_2 \geqslant a_1 - 1$, перейти к шагу H4.

H3. [Настройка a_1 и a_2.] Установить $a_1 \leftarrow a_1 - 1$, $a_2 \leftarrow a_2 + 1$ и вернуться к шагу H2.

H4. [Поиск j.] Установить $j \leftarrow 3$ и $s \leftarrow a_1 + a_2 - 1$. Затем, если $a_j \geqslant a_1 - 1$, установить $s \leftarrow s + a_j$, $j \leftarrow j + 1$ и повторять эти действия до тех пор, пока не будет выполнено условие $a_j < a_1 - 1$. (Теперь $s = a_1 + \cdots a_{j-1} - 1$.)

H5. [Увеличение a_j.] Завершить работу, если $j > m$. В противном случае установить $x \leftarrow a_j + 1$, $a_j \leftarrow x$, $j \leftarrow j - 1$.

H6. [Настройка $a_1 \ldots a_j$.] Пока $j > 1$, установить $a_j \leftarrow x$, $s \leftarrow s - x$ и $j \leftarrow j - 1$. В конце установить $a_1 \leftarrow s$ и вернуться к шагу H2. ▌

Например, при $n = 11$ и $m = 4$ посещаемые алгоритмом разбиения —

$$8111, 7211, 6311, 5411, 6221, 5321, 4421, 4331, 5222, 4322, 3332. \tag{7}$$

Основная идея состоит в том, что солексный порядок переходит от одного разбиения $a_1 \ldots a_m$ к другому путем поиска наименьшего j, такого, что a_j можно увеличить без изменения $a_{j+1} \ldots a_m$. Новое разбиение $a'_1 \ldots a'_m$ будет иметь $a'_1 \geqslant \cdots \geqslant a'_j = a_j + 1$ и $a'_1 + \cdots + a'_j = a_1 + \cdots + a_j$, и эти условия достижимы тогда и только тогда, когда $a_j < a_1 - 1$. Кроме того, наименьшее такое разбиение $a'_1 \ldots a'_m$ в солексном порядке имеет $a'_2 = \cdots = a'_j = a_j + 1$.

Шаг H3 обрабатывает простой случай $j = 2$, который наиболее распространен. Следует отметить, что значение j практически всегда достаточно мало́; позже мы докажем, что общее время работы алгоритма H не превышает количества посещенных разбиений, умноженного на небольшую константу, плюс $O(m)$.

Другие представления разбиений. Мы определили разбиение как последовательность неотрицательных целых чисел $a_1 a_2 \ldots$, обладающую теми свойствами, что $a_1 \geqslant a_2 \geqslant \cdots$ и $a_1 + a_2 + \cdots = n$, но можно также рассматривать его как n-кортеж неотрицательных целых чисел $c_1 c_2 \ldots c_n$, таких, что

$$c_1 + 2c_2 + \cdots + nc_n = n. \tag{8}$$

Здесь c_j — количество появлений числа j в последовательности $a_1 a_2 \ldots$; например, разбиение 331 соответствует количествам $c_1 = 1$, $c_2 = 0$, $c_3 = 2$, $c_4 = c_5 = c_6 = c_7 = 0$. Количество частей в таком случае составляет $c_1 + c_2 + \cdots + c_n$. Можно легко разработать процедуру, аналогичную алгоритму P, для генерации разбиений в виде количества частей (см. упражнение 5).

Мы уже встречались с неявным представлением в виде количества частей в формулах наподобие 1.2.9–(38), которые выражают симметричную функцию

$$h_n = \sum_{N \geqslant d_n \geqslant \cdots \geqslant d_2 \geqslant d_1 \geqslant 1} x_{d_1} x_{d_2} \ldots x_{d_n} \tag{9}$$

как

$$\sum_{\substack{c_1, c_2, \ldots, c_n \geqslant 0 \\ c_1 + 2c_2 + \cdots + nc_n = n}} \frac{S_1^{c_1}}{1^{c_1} c_1!} \frac{S_2^{c_2}}{2^{c_2} c_2!} \cdots \frac{S_n^{c_n}}{n^{c_n} c_n!}, \tag{10}$$

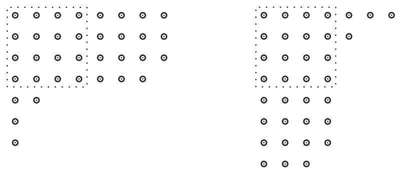
где S_j — симметричная функция $x_1^j + x_2^j + \cdots + x_N^j$. Сумма в (9), по сути, берется по всем n-мультисочетаниям N, в то время как сумма (10) берется по всем разбиениям

n. Таким образом, например, $h_3 = \frac{1}{6}S_1^3 + \frac{1}{2}S_1S_2 + \frac{1}{3}S_3$ и при $N = 2$ мы имеем

$$x^3 + x^2y + xy^2 + y^3 = \frac{1}{6}(x+y)^3 + \frac{1}{2}(x+y)\left(x^2+y^2\right) + \frac{1}{3}\left(x^3+y^3\right).$$

Другие суммы по всем разбиениям встречаются в упражнениях 1.2.5–21, 1.2.9–11, 1.2.10–12 и т.д.; по этой причине разбиения занимают важное место в изучении симметричных функций — класса функций, широко распространенного в математике. [Глава 7 работы Ричарда Стенли (Richard Stanley) *Enumerative Combinatorics*, **2** (1999) представляет собой превосходное введение в современные аспекты теории симметричных функций.]

Разбиения можно весьма привлекательно визуализировать, рассматривая массив из n точек, у которого a_1 точек в верхней строке, a_2 точек во второй строке и т.д. Такое размещение точек называется *диаграммой Ферререа* в честь Н.М. Феррерса (N.M. Ferrers) [*Philosophical Mag.*, **5** (1853), 199–202]; наибольший квадратный подмассив точек, содержащийся в такой диаграмме, называется *квадратом Дюрфи* по имени В.П. Дюрфи (W.P. Durfee) [*Johns Hopkins Univ. Circular*, **2** (December 1882), 23]. Например, на рис. 28, *а* показана диаграмма Феррерса для разбиения 8887211 с квадратом Дюрфи размером 4×4. Квадрат Дюрфи содержит k^2 точек, где k — наибольший индекс, такой, что $a_k \geqslant k$; можно называть k *следом* (trace) разбиения.



a) 8887211 b) 75444443

Рис. 28. Диаграмма Феррерса и квадрат Дюрфи двух сопряженных разбиений

Для произвольного разбиения α вида $a_1a_2\ldots$ *сопряженным* (conjugate) с ним является разбиение $\alpha^T = b_1b_2\ldots$, которое получается путем транспонирования строк и столбцов соответствующей диаграммы Феррерса. Например, на рис. 28, *b* показано, что $(8887211)^T = (75444443)$. Если $\beta = \alpha^T$, то очевидно, что $\alpha = \beta^T$; разбиение β имеет a_1 частей, а β — b_1 частей. Имеется простое соотношение между представлениями в виде количества частей $c_1\ldots c_n$ разбиения α и сопряженного разбиения $b_1b_2\ldots$, а именно:

$$b_j - b_{j+1} = c_j \quad \text{для всех } j \geqslant 1. \tag{11}$$

Это соотношение позволяет легко вычислить сопряженное для данного разбиения (см. упражнение 6).

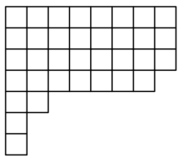
Понятие сопряженности часто поясняет свойства разбиений, которые иначе выглядели бы весьма загадочными. Например, теперь, зная определение α^T, мы можем легко увидеть, что значение $j-1$ на шаге H5 алгоритма H представляет собой вторую наименьшую часть сопряженного разбиения $(a_1\ldots a_m)^T$. Следовательно, среднее количество работы, которую необходимо выполнить на шагах H4 и H6, по сути, пропорционально среднему размеру второй наименьшей части случайного разбиения, наибольшая часть которого равна m. Ниже мы увидим, что эта вторая наименьшая часть почти всегда достаточно мала.

Кроме того, *алгоритм H выводит разбиения в лексикографическом порядке сопряженных к ним*. Например, соответствующими сопряженными к (7) являются

$$41111111, 4211111, 422111, 42221, 431111, 43211, 4322, 4331, 44111, 4421, 443; \qquad (12)$$

они представляют собой разбиения $n = 11$ с наибольшей частью, равной 4. Один из способов генерации всех разбиений n состоит в том, чтобы начать с тривиального разбиения 'n', затем поочередно применить алгоритм H для $m = 2, 3, \ldots, n$; такой процесс даст все α в лексикографическом порядке α^T (см. упражнение 7). Таким образом, алгоритм H можно рассматривать как дуальный к алгоритму P.

Имеется, как минимум, еще один способ представления разбиений, называющийся *краевым представлением* (rim representation). Предположим, что мы заменили точки на диаграмме Ферререса квадратами, получив таким образом подобие таблицы, как мы делали в разделе 5.1.4; например, разбиение 8887211 с рис. 28, *а* превращается в



(13)

Правая граница этого образа может рассматриваться как путь от нижнего левого угла в правый верхний угол квадрата размером $n \times n$, а из табл. 7.2.1.3–1 мы знаем, что такой путь соответствует (n, n)-сочетанию.

Например, (13) соответствует 70-битовой строке

$$0 \ldots 01001011111010001 \ldots 1 = 0^{28}1^1 0^2 1^1 0^1 1^5 0^1 1^1 0^3 1^{27}, \qquad (14)$$

в которой мы размещаем в начале достаточное количество нулей, а в конце — единиц, чтобы получить в точности по n каждых из них. Нули представляют шаги вверх, а единицы — вправо. Легко видеть, что определенная таким образом битовая строка имеет ровно n инверсий; и наоборот: каждая перестановка мультимножества $\{n \cdot 0, n \cdot 1\}$, которая содержит ровно n инверсий, соответствует разбиению n. Если разбиение имеет t различных частей, его битовая строка может быть записана в виде

$$0^{n-q_1-q_2-\cdots-q_t} 1^{p_1} 0^{q_1} 1^{p_2} 0^{q_2} \ldots 1^{p_t} 0^{q_t} 1^{n-p_1-p_2-\cdots-p_t}, \qquad (15)$$

где показатели степени p_j и q_j представляют собой положительные целые числа. В таком случае стандартным представлением разбиения является

$$a_1 a_2 \ldots = (p_1 + \cdots + p_t)^{q_t} \, (p_1 + \cdots + p_{t-1})^{q_{t-1}} \cdots (p_1)^{q_1}\,, \qquad (16)$$

т.е. в нашем примере $(1 + 1 + 5 + 1)^3 \, (1 + 1 + 5)^1 \, (1 + 1)^1 \, (1)^2 = 8887211$.

Количество разбиений. Вопрос, заданный в 1740 году Филиппом Ноде (Philipp Naudé), побудил Леонарда Эйлера (Leonhard Euler) написать две фундаментальные статьи, в которых он подсчитывал количества разбиений различного вида, изучая их производящие функции [*Commemtarii Academiaæ Scientiarum Petropolitanæ*, **13** (1741), 64–93; *Novi Comment. Acad. Sci. Pet.*, **3** (1750), 125–169]. Он заметил, что коэффициент при z^n в бесконечном произведении

$$\left(1+z+z^2+\cdots+z^j+\cdots\right)\left(1+z^2+z^4+\cdots+z^{2k}+\cdots\right)$$
$$\left(1+z^3+z^6+\cdots+z^{3l}+\cdots\right)\ldots$$

равен количеству неотрицательных целых решений уравнения $j+2k+3l+\cdots=n$; а $1+z^m+z^{2m}+\cdots$ равно $1/(1-z^m)$. Следовательно, если мы запишем

$$P(z)=\prod_{m=1}^{\infty}\frac{1}{1-z^m}=\sum_{n=0}^{\infty}p(n)\,z^n, \tag{17}$$

то количество разбиений n равно $p(n)$. Функция $P(z)$, в свою очередь, обладает рядом поразительных математических свойств.

Например, Эйлер открыл наличие большого количества сокращений при раскрытии скобок знаменателя $P(z)$:

$$(1-z)\left(1-z^2\right)\left(1-z^3\right)\ldots=1-z-z^2+z^5+z^7-z^{12}-z^{15}+z^{22}+z^{26}-\cdots=$$
$$=\sum_{-\infty<n<\infty}(-1)^n\,z^{\left(3n^2+n\right)/2}. \tag{18}$$

Комбинаторное доказательство этого замечательного тождества, основанное на диаграммах Ферререса, имеется в упражнении 5.1.1–14; можно также доказать его, положив $u=z$ и $v=z^2$ в еще более замечательном тождестве Якоби

$$\prod_{k=1}^{\infty}\left(1-u^kv^{k-1}\right)\left(1-u^{k-1}v^k\right)\left(1-u^kv^k\right)=\sum_{n=-\infty}^{\infty}(-1)^n\,u^{\binom{n}{2}}v^{\binom{-n}{2}}, \tag{19}$$

поскольку левая часть при этом становится равной

$$\prod_{k=1}^{\infty}\left(1-z^{3k-2}\right)\left(1-z^{3k-1}\right)\left(1-z^{3k}\right);$$

см. упражнение 5.1.1–20. Из тождества Эйлера (18) вытекает, что количество разбиений удовлетворяет рекуррентному соотношению

$$p(n)=p(n-1)+p(n-2)-p(n-5)-p(n-7)+p(n-12)+p(n-15)-\cdots, \tag{20}$$

на основании которого можно вычислить соответствующие значения быстрее, чем выполняя вычисление степенных рядов (17).

n	=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$p(n)$	=	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176

Из раздела 1.2.8 мы знаем, что решение рекуррентного соотношения Фибоначчи $f(n)=f(n-1)+f(n-2)$ при положительных $f(0)$ и $f(1)$ растет экспоненциально: $f(n)=\Theta(\phi^n)$. Дополнительные члены '$-p(n-5)-p(n-7)$' в (20) оказывают подавляющее влияние на количество разбиений; более того, если ограничиться в рекуррентном соотношении только этими членами, полученный в результате ряд осциллирует между положительными и отрицательными значениями. Следующие члены, '$+p\,(n-12)+p\,(n-15)$', восстанавливают экспоненциальный рост.

Реальная скорость роста $p\,(n)$ имеет порядок $A^{\sqrt{n}}/n$ для некоторой константы A. Например, в упражнении 33 доказывается, что $p\,(n)$ растет со скоростью, как минимум, $e^{2\sqrt{n}}/n$. Еще один простой способ получить неплохую *верхнюю* границу состоит в логарифмировании (17)

$$\ln P\,(z) = \sum_{m=1}^{\infty} \ln \frac{1}{1-z^m} = \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} \frac{z^{mn}}{n}; \tag{21}$$

затем следует рассмотреть его поведение вблизи $z=1$, положив $z=e^{-t}$:

$$\ln P\left(e^{-t}\right) = \sum_{m,n\geqslant 1} \frac{e^{-mnt}}{n} = \sum_{n\geqslant 1} \frac{1}{n}\frac{1}{e^{tn}-1} < \sum_{n\geqslant 1} \frac{1}{n^2 t} = \frac{\zeta\,(2)}{t}. \tag{22}$$

Далее, поскольку $p\,(n) \leqslant p\,(n+1) < p\,(n+2) < \cdots$ и $e^t > 1$, получаем

$$\frac{p\,(n)}{1-e^{-t}} < \sum_{k=0}^{\infty} p\,(k)\,e^{(n-k)t} = e^{nt}P\left(e^{-t}\right) < e^{nt+\zeta(2)/t} \tag{23}$$

для всех $t>0$. Приравнивание $t=\sqrt{\zeta\,(2)/n}$ дает

$$p\,(n) < Ce^{2C\sqrt{n}}/\sqrt{n}, \text{ где } C = \sqrt{\zeta\,(2)} = \pi/\sqrt{6}. \tag{24}$$

Более точную информацию о величине $\ln P\,(e^{-t})$ можно получить, воспользовавшись формулой суммирования Эйлера (раздел 1.2.11.2) или преобразованием Меллина (раздел 5.2.2); см. упражнение 25. Однако рассмотренные методы недостаточно мощны для определения точного поведения $P\,(e^{-t})$, так что самое время добавить в наш арсенал новые методы.

Производящая функция Эйлера $P\,(z)$ идеально подходит для *формулы суммирования Пуассона* [*J. École Royale Polytechnique*, **12** (1823), 404–509, § 63], в соответствии с которой

$$\sum_{n=-\infty}^{\infty} f\,(n+\theta) = \lim_{M\to\infty} \sum_{m=-M}^{M} e^{2\pi mi\theta} \int_{-\infty}^{\infty} e^{-2\pi miy} f\,(y)\,dy, \tag{25}$$

где f — "хорошо себя ведущая" функция. Эта формула основана на том факте, что в левой части находится периодическая функция от θ, а в правой — ее разложение в ряд Фурье. Функция f достаточно хорошая, если, например, $\int_{-\infty}^{\infty} |f\,(y)|\,dy < \infty$, а также

i) либо $f\,(n+\theta)$ является аналитической функцией комплексной переменной θ в области $|\Im\theta| \leqslant \varepsilon$ для некоторого $\varepsilon > 0$ и $0 \leqslant \Re\theta \leqslant 1$, и левая часть равномерно сходится в этом прямоугольнике;

ii) либо $f\,(\theta) = \frac{1}{2}\lim_{\varepsilon\to 0}\left(f\,(\theta-\varepsilon)+f\,(\theta+\varepsilon)\right) = g\,(\theta) - h\,(\theta)$ для всех действительных чисел θ, где g и h — монотонно возрастающие, а $g\,(\pm\infty)$ и $h\,(\pm\infty)$ конечны.

[Peter Henrici, *Applied and Computational Complex Analysis*, **2** (New York: Wiley, 1977), Theorem 10.6.2.] Формула Пуассона не панацея для задач суммирования любого вида, но если она применима, то ее результаты, как мы увидим, могут быть впечатляющи.

Умножим формулу Эйлера (18) на $z^{1/24}$ для "завершения квадрата":

$$\frac{z^{1/24}}{P(z)} = \sum_{n=-\infty}^{\infty} (-1)^n \, z^{\frac{3}{2}\left(n+\frac{1}{6}\right)^2}. \tag{26}$$

Тогда для всех $t > 0$ имеем $e^{-t/24}/P(e^{-t}) = \sum_{n=-\infty}^{\infty} f(n)$, где

$$f(y) = e^{-\frac{3}{2}t\left(y+\frac{1}{6}\right)^2} \cos \pi y; \tag{27}$$

и эта функция f подходит для формулы суммирования Пуассона, так как удовлетворяет обоим критериям, приведенным выше. Таким образом, мы можем попытаться проинтегрировать $e^{-2\pi miy} f(y)$ и для $m = 0$ получить результат

$$\int_{-\infty}^{\infty} f(y)\, dy = \sqrt{\frac{\pi}{2t}} e^{-\pi^2/6t}. \tag{28}$$

К этому мы должны добавить

$$\sum_{m=1}^{\infty} \int_{-\infty}^{\infty} \left(e^{2\pi miy} + e^{-2\pi miy}\right) f(y)\, dy = 2 \sum_{m=1}^{\infty} \int_{-\infty}^{\infty} f(y) \cos 2\pi my \, dy; \tag{29}$$

этот интеграл также оказывается берущимся. Будучи объединены, все результаты (см. упражнение 27) дают

$$\frac{e^{-t/24}}{P(e^{-t})} = \sqrt{\frac{2\pi}{t}} \sum_{n=-\infty}^{\infty} (-1)^n \, e^{-6\pi^2\left(n+\frac{1}{6}\right)^2/t} = \sqrt{\frac{2\pi}{t}} \, \frac{e^{-\pi^2/6t}}{P\left(e^{-4\pi^2/t}\right)}. \tag{30}$$

Небольшой сюрприз — мы доказали еще один замечательный факт о $P(z)$ — приведенную далее теорему.

Теорема D. *Производящая функция (17) для разбиений удовлетворяет функциональному соотношению*

$$\ln P\left(e^{-t}\right) = \frac{\zeta(2)}{t} + \frac{1}{2} \ln \frac{t}{2\pi} - \frac{t}{24} + \ln P\left(e^{-4\pi^2/t}\right) \tag{31}$$

при $\Re t > 0$. ∎

Эта теорема была открыта Дедекиндом (Dedekind) [*Crelle*, **83** (1877), 265–292, § 6], который для функции $z^{1/24}/P(z)$ использовал запись $\eta(\tau)$, где $z = e^{2\pi i\tau}$; его доказательство основано на существенно более сложной теории эллиптических функций. Заметим, что, когда t — малое положительное число, $\ln P\left(e^{-4\pi^2/t}\right)$ ***крайне*** мало́; например, при $t = 0.1$ получаем $\exp\left(-4\pi^2/t\right) \approx 3.5 \times 10^{-172}$. Таким образом, теорема D дает нам практически все, что необходимо знать о значении $P(z)$ при z, близком к 1.

Г.Г. Харди (G.H. Hardy) и С. Рамануджан (S. Ramanujan) использовали это знание для вывода асимптотического поведения $p(n)$ при больших n, и их работа была продолжена многие годы спустя Х. Радемахером (H. Rademacher), открывшим ряд, который не только асимптотичен, но и сходится [*Proc. London Math. Soc.* (2), **17** (1918), 75–115; **43** (1937), 241–254]. Формула Харди–Рамануджана–Радемахера для $p(n)$ поистине одно из наиболее изумительных тождеств; она гласит, что

$$p(n)=\frac{\pi}{2^{5/4}3^{3/4}(n-1/24)^{3/4}}\sum_{k=1}^{\infty}\frac{A_k(n)}{k}I_{3/2}\left(\sqrt{\frac{2}{3}}\frac{\pi}{k}\sqrt{n-1/24}\right). \tag{32}$$

Здесь $I_{3/2}$ означает модифицированную сферическую функцию Бесселя

$$I_{3/2}(z)=\left(\frac{z}{2}\right)^{3/2}\sum_{k=0}^{\infty}\frac{1}{\Gamma(k+5/2)}\frac{\left(z^2/4\right)^k}{k!}=\sqrt{\frac{2z}{\pi}}\left(\frac{\cosh z}{z}-\frac{\sinh z}{z^2}\right), \tag{33}$$

а коэффициент $A_k(n)$ определяется формулой

$$A_k(n)=\sum_{h=0}^{k-1}[h\perp k]\exp\left(2\pi i\left(\frac{\sigma(h,k,0)}{24}-\frac{nh}{k}\right)\right), \tag{34}$$

где $\sigma(h,k,0)$ — сумма Дедекинда, определенная в уравнении 3.3.3–(16). В результате

$$A_1(n)=1,\quad A_2(n)=(-1)^n,\quad A_3(n)=2\cos\frac{(24n+1)\pi}{18}, \tag{35}$$

и в общем случае$A_k(n)$ лежит между $-k$ и k.

Доказательство (32) может увести нас слишком далеко, но основная идея состоит в использовании "метода седловой точки", рассматривающегося в разделе 7.2.1.5. Член для $k=1$ выводится из поведения $P(z)$ при z, близком к 1; следующий член выводится из поведения z вблизи -1, здесь можно применить преобразование, подобное (31). В общем случае k-й член (32) учитывает поведение $P(z)$ при z, стремящемся к $e^{2\pi ih/k}$ для несократимых дробей h/k со знаменателем k; каждый k-й корень единицы представляет собой полюс для каждой из дробей $1/\left(1-z^k\right)$, $1/\left(1-z^{2k}\right)$, $1/\left(1-z^{3k}\right)$, … в бесконечном произведении $P(z)$.

Старший член (32) может быть существенно упрощен, если нам достаточно грубого приближения:

$$p(n)=\frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}\left(1+O\left(n^{-1/2}\right)\right). \tag{36}$$

Если же такой точности недостаточно, можно воспользоваться более детальным приближением:

$$p(n)=\frac{e^{\pi\sqrt{2n'/3}}}{4n'\sqrt{3}}\left(1-\frac{1}{\pi}\sqrt{\frac{3}{2n'}}\right)\left(1+O\left(e^{-\pi\sqrt{n/6}}\right)\right),\quad n'=n-\frac{1}{24}. \tag{37}$$

Например, $p(100)$ имеет точное значение 190 569 292; формула (36) дает нам $p(100)\approx$ $\approx 1.993\times10^8$, в то время как (37) — гораздо лучшую оценку 190 568 944.783.

Э. Одлызко (A. Odlyzko) заметил, что при больших n формула Харди–Рамануджана–Радемахера дает близкий к оптимальному способ вычисления точного значения $p(n)$, поскольку арифметические операции могут быть выполнены примерно за $O(\log p(n)) = O\left(n^{1/2}\right)$ шагов. Основной вклад вносят несколько первых членов (32); затем ряд стремится к членам, не превышающим порядка $k^{-3/2}$, обычно порядка k^{-2}. Кроме того, около половины коэффициентов $A_k(n)$ оказываются равными 0 (см. упражнение 28). Например, при $n = 10^6$ члены для $k = 1, 2, 3$ приблизительно равны 1.47×10^{1107}, 1.23×10^{550} и -1.23×10^{364} соответственно. Сумма первых 250 членов приближенно равна 1471684986…73818.01, в то время как истинное значение равно 1471684986…73818; при этом 123 из 250 членов равны нулю.

Количество частей. Удобно ввести обозначение

$$\left|{n \atop m}\right| \tag{38}$$

для количества разбиений n, состоящих ровно из m частей. Тогда для всех целых m и n выполняется рекуррентное соотношение

$$\left|{n \atop m}\right| = \left|{n-1 \atop m-1}\right| + \left|{n-m \atop m}\right|, \tag{39}$$

поскольку $\left|{n-1 \atop m-1}\right|$ подсчитывает разбиения, наименьшая часть которых равна 1, а $\left|{n-m \atop m}\right|$ — прочие разбиения. (Если наименьшая часть равна 2 или больше, мы можем вычесть 1 из каждой части и получить разбиение $n-m$ на m частей.) Аналогичные рассуждения приводят к заключению, что $\left|{m+n \atop m}\right|$ — количество разбиений n на *не более* чем m частей, а именно на m неотрицательных слагаемых. Мы также знаем из транспонирования диаграмм Феррерса, что $\left|{n \atop m}\right|$ представляет собой количество разбиений n, у которых *наибольшая* часть равна m. Таким образом, $\left|{n \atop m}\right|$ — число, которое стоит того, чтобы его изучить. Граничные условия

$$\left|{n \atop 0}\right| = \delta_{n0} \text{ и } \left|{n \atop m}\right| = 0 \text{ для } m < 0 \text{ или } n < 0 \tag{40}$$

делают простой табуляцию $\left|{n \atop m}\right|$ для небольших значений параметров, и мы можем получить массив чисел аналогично знакомым треугольникам для $\binom{n}{m}$, $\left[{n \atop m}\right]$, $\left\{{n \atop m}\right\}$ и $\left\langle{n \atop m}\right\rangle$, с которыми мы встречались ранее (табл. 2). Производящая функция имеет вид

$$\sum_n \left|{n \atop m}\right| z^n = \frac{z^m}{(1-z)(1-z^2)\ldots(1-z^m)}. \tag{41}$$

Почти все разбиения n состоят из $\Theta(\sqrt{n}\log n)$ частей. Этот факт, открытый П. Эрдешем (P. Erdős) и Д. Ленером (J. Lehner) [*Duke Math. J.*, **8** (1941), 335–345], имеет весьма поучительное доказательство.

Теорема E. *Пусть* $C = \pi/\sqrt{6}$ *и* $m = \frac{1}{2C}\sqrt{n}\ln n + x\sqrt{n} + O(1)$. *Тогда*

$$\frac{1}{p(n)}\left|{m+n \atop n}\right| = F(x)\left(1 + O\left(n^{-1/2+\varepsilon}\right)\right) \tag{42}$$

Таблица 2. Количества разбиений

n	$\left\|{n \atop 0}\right\|$	$\left\|{n \atop 1}\right\|$	$\left\|{n \atop 2}\right\|$	$\left\|{n \atop 3}\right\|$	$\left\|{n \atop 4}\right\|$	$\left\|{n \atop 5}\right\|$	$\left\|{n \atop 6}\right\|$	$\left\|{n \atop 7}\right\|$	$\left\|{n \atop 8}\right\|$	$\left\|{n \atop 9}\right\|$	$\left\|{n \atop 10}\right\|$	$\left\|{n \atop 11}\right\|$
0	1	0	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0	0	0	0	0
3	0	1	1	1	0	0	0	0	0	0	0	0
4	0	1	2	1	1	0	0	0	0	0	0	0
5	0	1	2	2	1	1	0	0	0	0	0	0
6	0	1	3	3	2	1	1	0	0	0	0	0
7	0	1	3	4	3	2	1	1	0	0	0	0
8	0	1	4	5	5	3	2	1	1	0	0	0
9	0	1	4	7	6	5	3	2	1	1	0	0
10	0	1	5	8	9	7	5	3	2	1	1	0
11	0	1	5	10	11	10	7	5	3	2	1	1

для всех $\varepsilon > 0$ *и всех фиксированных* x *при* $n \to \infty$, *где*

$$F(x) = e^{-e^{-Cx}/C}. \tag{43}$$

Эта функция $F(x)$ достаточно быстро стремится к 0 при $x \to -\infty$ и быстро возрастает до 1 при $x \to +\infty$; таким образом, это функция распределения вероятностей. На рис. 29, *б* показана соответствующая функция плотности распределения вероятностей $f(x) = F'(x)$, которая сосредоточена в основном в области $-2 \leqslant x \leqslant 4$. Для сравнения на рис. 29, *а* показаны значения $\left|{n \atop m}\right| = \left|{m+n \atop m}\right| - \left|{m-1+n \atop m-1}\right|$ при $n = 100$; в этом случае $\frac{1}{2C}\sqrt{n}\ln n \approx 18$.

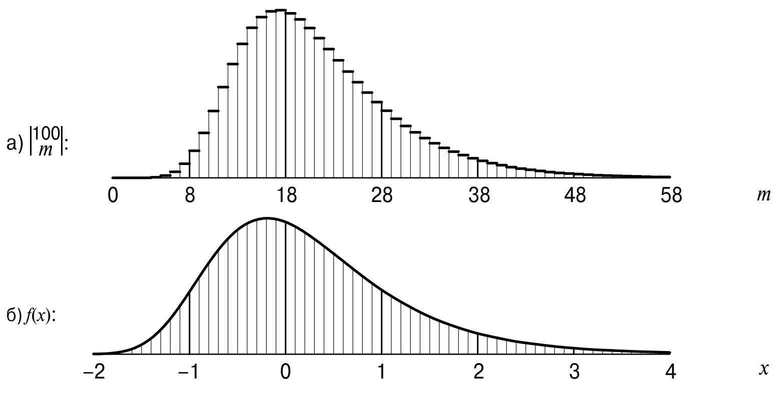


Рис. 29. Разбиения n на m частей, при *а*) $n = 100$; *б*) $n \to \infty$ (см. теорему E)

Доказательство. Воспользуемся тем фактом, что $\left|{m+n \atop m}\right|$ — количество разбиений n, у которых бо́льшая часть $\leqslant m$. Тогда, согласно принципу включения и исключения (формула 1.3.3–(29)), имеем

$$\left|{m+n \atop m}\right| = p(n) - \sum_{j>m} p(n-j) + \sum_{j_2>j_1>m} p(n-j_1-j_2) - \\ - \sum_{j_3>j_2>j_1>m} p(n-j_1-j_2-j_3) + \cdots,$$

поскольку $p(n-j_1-\cdots-j_r)$ — количество разбиений n, которые используют каждую из частей $\{j_1,\ldots,j_r\}$ хотя бы один раз. Запишем это как

$$\frac{1}{p(n)}\left|{m+n \atop m}\right| = 1-\Sigma_1+\Sigma_2-\Sigma_3+\cdots, \quad \Sigma_r = \sum_{j_r>\cdots>j_1>m}\frac{p(n-j_1-\cdots-j_r)}{p(n)}. \quad (44)$$

Для того чтобы вычислить Σ_r, нам нужна хорошая оценка отношения $\frac{p(n-t)}{p(n)}$. Нам везет, поскольку из (36) вытекает, что

$$\frac{p(n-t)}{p(n)} = \exp\left(2C\sqrt{n-t}-\ln(n-t)+O\left((n-t)^{-1/2}\right)-2C\sqrt{n}+\ln n\right) = \\ = \exp\left(-Ctn^{-1/2}+O\left(n^{-1/2+2\varepsilon}\right)\right) \text{ при } 0\leqslant t\leqslant n^{1/2+\varepsilon}. \quad (45)$$

Далее, если $t\geqslant n^{1/2+\varepsilon}$, мы имеем $p(n-t)/p(n)\leqslant p\left(n-n^{1/2+\varepsilon}\right)/p(n)\approx\exp(-Cn^{\varepsilon})$, значение, которое асимптотически меньше, чем любая степень n. Следовательно, мы безопасно можем использовать приближение

$$\frac{p(n-t)}{p(n)}\approx\alpha^t, \qquad \alpha=\exp\left(-Cn^{-1/2}\right), \quad (46)$$

для всех значений $t\geqslant 0$. Например, мы имеем

$$\Sigma_1 = \sum_{j>m}\frac{p(n-j)}{p(n)} = \frac{\alpha^{m+1}}{1-\alpha}\left(1+O\left(n^{-1/2+2\varepsilon}\right)\right)+\sum_{n\geqslant j>n^{1/2+\varepsilon}}\frac{p(n-j)}{p(n)} = \\ = \frac{e^{-Cx}}{C}\left(1+O\left(n^{-1/2+2\varepsilon}\right)\right)+O\left(ne^{-Cn^{\varepsilon}}\right),$$

поскольку $\alpha/(1-\alpha) = n^{1/2}/C+O(1)$ и $\alpha^m = n^{-1/2}e^{-Cx}$. Аналогичные доводы (см. упражнение 36) доказывают, что при $r=O(\log n)$

$$\Sigma_r = \frac{e^{-Crx}}{C^r r!}\left(1+O\left(n^{-1/2+2\varepsilon}\right)\right)+O\left(e^{-n^{\varepsilon/2}}\right). \quad (47)$$

Наконец — и это замечательное свойство принципа включения-исключения в общем случае — частичные суммы (44) всегда “берут в вилку” истинное значение, в том смысле, что

$$1-\Sigma_1+\Sigma_2-\cdots-\Sigma_{2r-1}\leqslant\frac{1}{p(n)}\left|{m+n \atop m}\right|\leqslant 1-\Sigma_1+\Sigma_2-\cdots-\Sigma_{2r-1}+\Sigma_{2r} \quad (48)$$

при всех r (см. упражнение 37). Когда $2r$ близко к $\ln n$ и n велико, член Σ_{2r} чрезвычайно мал; таким образом, мы получаем (42), за исключением того, что вместо ε используется 2ε. ▮

Теорема E говорит о том, что наибольшая часть случайного разбиения почти всегда представляет собой $\frac{1}{2C}\sqrt{n}\ln n + O(\sqrt{n})$ и при достаточно большом n остальные части также имеют тенденцию к предсказуемости. Предположим, например, что мы берем все разбиения числа 25 и накладываем одну на другую их диаграммы Ферререса, заменяя точки квадратами, как в случае краевого представления. Какие ячейки будут заниматься наиболее часто? На рис. 30 показан результат: случайное разбиение стремится к типичному виду, приближающемуся к предельной кривой при $n \to \infty$.

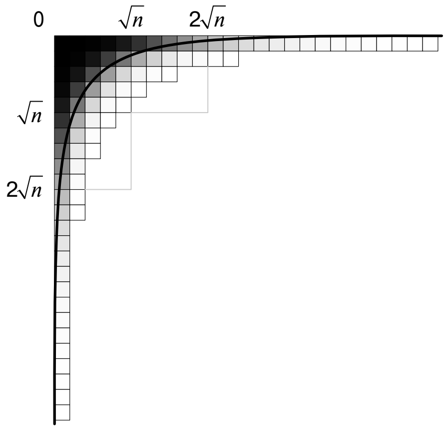


Рис. 30. Кривая Темперли (49), ограничивающая случайное разбиение

Г. Темперли (H. Temperley) [*Proc. Cambridge Philos. Soc.*, **48** (1952), 683–697] привел эвристические обоснования того, что основные части a_k большого случайного разбиения $a_1 \ldots a_m$ будут удовлетворять приближенному закону

$$e^{-Ck/\sqrt{n}} + e^{-Ca_k/\sqrt{n}} \approx 1, \tag{49}$$

и его формула была впоследствии подтверждена в строгом виде. Например, теорема Б. Питтеля [*Advanced in Applied Math.*, **18** (1997), 432–488] позволяет нам заключить, что след случайного разбиения почти всегда равен $\frac{\ln 2}{C}\sqrt{n} \approx 0.54\sqrt{n}$, что согласуется с (49) с ошибкой не более $O(\sqrt{n}\ln n)^{1/2}$; таким образом, около 29% всех точек Ферререса лежат в пределах квадрата Дюрфи.

С другой стороны, если мы рассмотрим только разбиения n на m частей, где m — фиксированная величина, ограничивающая кривая будет иной: почти все разбиения имеют

$$a_k \approx \frac{n}{m} \ln \frac{m}{k} \tag{50}$$

при достаточно большом m. На рис. 31 показан случай $n = 50$, $m = 5$. В действительности тот же предел справедлив при m, растущем с ростом n, но со скоростью, меньшей $\sqrt{n}$ [см. А. Вершик и Ю. Якубович, *Moscow Math. J.*, **1** (2001), 457–468].

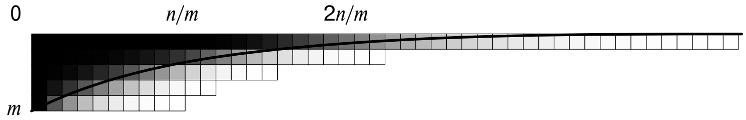


Рис. 31. Ограничивающая кривая (50) при наличии m частей

Краевое представление разбиений дает нам дальнейшую информацию о *дважды* ограниченных разбиениях, когда ограничено не только количество частей, но и размер каждой части. Разбиение, которое имеет не более m частей, каждая из которых не превосходит l, располагается в пределах прямоугольника $m \times l$. Все такие разбиения соответствуют перестановкам мультимножества $\{m \cdot 0, l \cdot 1\}$, имеющим ровно n инверсий; инверсии перестановок мультимножества мы уже изучали в упражнении 5.1.2–16. В частности, в упомянутом упражнении выводится неочевидная формула для количества способов получения n инверсий.

Теорема C. *Количество разбиений n, которые состоят не более чем из m частей, не превышающих по размеру l, равно*

$$[z^n]\binom{l+m}{m}_z = [z^n]\,\frac{(1-z^{l+1})}{(1-z)}\frac{(1-z^{l+2})}{(1-z^2)}\cdots\frac{(1-z^{l+m})}{(1-z^m)}. \qquad (51)$$

Этот результат получен А. Коши (A. Cauchy) [*Comptes Rendus Acad. Sci.*, **17** (Paris, 1843), 523–531]. Обратите внимание, что при $n \to \infty$ числитель становится равным просто 1. Интересное комбинаторное доказательство более общего результата приведено в упражнении 39. ∎

Анализ алгоритмов. Теперь мы знаем более чем достаточно о количественных аспектах разбиений, чтобы с высокой степенью точности вывести поведение алгоритма P. Предположим, что шаги P1, ..., P6 этого алгоритма выполняются соответственно $T_1(n), \ldots, T_6(n)$ раз. Очевидно, что $T_1(n) = 1$ и $T_3(n) = p(n)$; из закона Киргофа вытекает, что $T_2(n) = T_5(n)$ и $T_4(n) + T_5(n) = T_3(n)$. Мы переходим к шагу P4 по одному разу для каждого разбиения, содержащего 2; понятно, что это происходит $p(n-2)$ раз.

Таким образом, единственная возможная загадка алгоритма P — количество выполнений шага P6, в котором возможен переход к самому себе. Однако небольшое размышление открывает нам, что алгоритм сохраняет значение $\geqslant 2$ в массиве $a_1 a_2 \ldots$ только на шагах P2 и P6; и каждое такое значение в конечном итоге уменьшается на 1 либо на шаге P4, либо на шаге P5. Следовательно,

$$T_2''(n) + T_6(n) = p(n) - 1, \qquad (52)$$

где $T_2''(n)$ — количество раз, когда шаг P2 устанавливает a_m равным значению $\geqslant 2$. Пусть $T_2(n) = T_2'(n) + T_2''(n)$, так что $T_2'(n)$ — количество раз, когда шаг P2 устанавливает $a_m \leftarrow 1$. Тогда $T_2'(n) + T_4(n)$ — количество разбиений, заканчивающихся на 1, следовательно,

$$T_2'(n) + T_4(n) = p(n-1). \qquad (53)$$

Итак, мы получили достаточное количество уравнений, чтобы определить все искомые величины:

$$(T_1(n), \ldots, T_6(n)) = \\ = (1, p(n) - p(n-2), p(n), p(n-2), p(n) - p(n-2), p(n-1) - 1). \quad (54)$$

Из асимптотики $p(n)$ мы также знаем среднее количество вычислений на одно разбиение:

$$\left(\frac{T_1(n)}{p(n)}, \ldots, \frac{T_6(n)}{p(n)}\right) = \left(0, \frac{2C}{\sqrt{n}}, 1, 1 - \frac{2C}{\sqrt{n}}, \frac{2C}{\sqrt{n}}, 1 - \frac{C}{\sqrt{n}}\right) + O\left(\frac{1}{n}\right), \quad (55)$$

где $C = \pi/\sqrt{6} \approx 1.283$ (см. упражнение 45). Общее количество обращений к памяти на одно разбиение составляет, таким образом, $4 - 3C/\sqrt{n} + O(1/n)$.

Если кто-то захочет сгенерировать все разбиения, он не только должен выполнить непомерную работу, но и быть безмерно внимательным, чтобы не ошибиться.
— Леонард Эйлер (Leonard Euler),
Разбиение чисел (De Partitione Numerorum) (1750)

Алгоритм A более сложен для анализа, но мы можем, как минимум, доказать верхнюю границу времени его работы. Ключевой величиной является значение j, наименьшего индекса, для которого $a_j < a_1 - 1$. Последовательные значения j для $m = 4$ и $n = 11$ равны $(2, 2, 2, 3, 2, 2, 3, 4, 2, 3, 5)$, и мы замечаем, что $j = b_{l-1} + 1$, где $b_1 \ldots b_l$ — сопряженное разбиение $(a_1 \ldots a_m)^T$ (см. (7) и (12)). Шаг H3 выделяет случай $j = 2$, поскольку он не только наиболее часто встречается, но и очень легко обрабатывается.

Пусть $c_m(n)$ — суммарное общее значение $j - 1$, просуммированное по всем $\left|{n \atop m}\right|$ разбиениям, сгенерированным алгоритмом H. Например, $c_4(11) = 1 + 1 + 1 + 2 + + 1 + 1 + 2 + 3 + 1 + 2 + 4 = 19$. Мы можем рассматривать $c_m(n)/\left|{n \atop m}\right|$ как хороший показатель времени работы на одно разбиение, поскольку время работы наиболее трудоемких шагов H4 и H6 грубо пропорционально $j - 2$. Это отношение $c_m(n)/\left|{n \atop m}\right|$ *не* ограниченно, поскольку $c_m(m) = m$, в то время как $\left|{m \atop m}\right| = 1$. Однако следующая теорема показывает, что алгоритм H достаточно эффективен.

Теорема H. *Мера стоимости $c_m(n)$ алгоритма H не превышает $3\left|{n \atop m}\right| + m$.*

Доказательство. Мы можем легко проверить, что $c_m(n)$ удовлетворяет тому же рекуррентному соотношению, что и $\left|{n \atop m}\right|$, а именно

$$c_m(n) = c_{m-1}(n-1) + c_m(n-m) \quad \text{для } m, n \geqslant 1, \quad (56)$$

если мы искусственно определим $c_m(n) = 1$ при $1 \leqslant n < m$ (см. (39)). Однако граничные условия теперь иные:

$$c_m(0) = [m > 0]; \qquad c_0(n) = 0. \quad (57)$$

В табл. 3 показано поведение $c_m(n)$ при малых m и n.

Таблица 3. Стоимости алгоритма H

n	$c_0(n)$	$c_1(n)$	$c_2(n)$	$c_3(n)$	$c_4(n)$	$c_5(n)$	$c_6(n)$	$c_7(n)$	$c_8(n)$	$c_9(n)$	$c_{10}(n)$	$c_{11}(n)$
0	0	1	1	1	1	1	1	1	1	1	1	1
1	0	1	1	1	1	1	1	1	1	1	1	1
2	0	1	2	1	1	1	1	1	1	1	1	1
3	0	1	2	3	1	1	1	1	1	1	1	1
4	0	1	3	3	4	1	1	1	1	1	1	1
5	0	1	3	4	4	5	1	1	1	1	1	1
6	0	1	4	6	5	5	6	1	1	1	1	1
7	0	1	4	7	7	6	6	7	1	1	1	1
8	0	1	5	8	11	8	7	7	8	1	1	1
9	0	1	5	11	12	12	9	8	8	9	1	1
10	0	1	6	12	16	17	13	10	9	9	10	1
11	0	1	6	14	19	21	18	14	11	10	10	11

Для доказательства теоремы мы докажем на самом деле более строгий результат:

$$c_m(n) \leqslant 3\left|\begin{matrix} n \\ m \end{matrix}\right| + 2m - n - 1 \text{ при } n \geqslant m \geqslant 2. \tag{58}$$

В упражнении 50 показано, что это неравенство выполняется при $m \leqslant n \leqslant 2m$, а значит, доказательство будет завершено, если мы докажем его для $n > 2m$. В этом случае по индукции мы имеем

$$\begin{aligned} c_m(n) &= c_1(n-m) + c_2(n-m) + c_3(n-m) + \cdots + c_m(n-m) \leqslant \\ &\leqslant 1 + \left(3\left|\begin{matrix} n-m \\ 2 \end{matrix}\right| + 3 - n + m\right) + \left(3\left|\begin{matrix} n-m \\ 3 \end{matrix}\right| + 5 - n + m\right) + \cdots + \\ &\qquad + \left(3\left|\begin{matrix} n-m \\ m \end{matrix}\right| + 2m - 1 - n + m\right) = \\ &= 3\left|\begin{matrix} n-m \\ 1 \end{matrix}\right| + 3\left|\begin{matrix} n-m \\ 2 \end{matrix}\right| + \cdots + 3\left|\begin{matrix} n-m \\ m \end{matrix}\right| - 3 + m^2 - (m-1)(n-m) = \\ &= 3\left|\begin{matrix} n \\ m \end{matrix}\right| + 2m^2 - m - (m-1)n - 3; \end{aligned}$$

а $2m^2 - m - (m-1)n - 3 \leqslant 2m - n - 1$, так как $n \geqslant 2m + 1$. ∎

***Код Грея для разбиений.** При генерации разбиений в виде количества частей $c_1 \ldots c_n$ (как в упражнении 5) на каждом шаге изменяется не более четырех значений c_j. Однако мы можем предпочесть минимизировать изменения отдельных частей, генерируя разбиения таким образом, чтобы следующее за $a_1 a_2 \ldots a_n$ разбиение получалось простой установкой $a_j \leftarrow a_j + 1$ и $a_k \leftarrow a_k - 1$ для некоторых j и k, как в алгоритме двери-вертушки в разделе 7.2.1.3. Это оказывается всегда возможным; для $n = 6$ имеется единственный способ такой генерации:

$$111111, 21111, 3111, 2211, 222, 321, 33, 42, 411, 51, 6. \tag{59}$$

В общем случае $\left|{n+m \atop m}\right|$ разбиений n не более чем на m частей всегда могут быть сгенерированы подходящим путем Грея.

Заметим, что $\alpha \to \beta$ — допустимый переход от одного разбиения к другому тогда и только тогда, когда мы получаем диаграмму Феррерса для β путем перемещения только одной точки в диаграмме Феррерса для α. Таким образом, $\alpha^T \to \beta^T$ также является допустимым переходом. Отсюда следует, что каждый код Грея для разбиения не более чем на m частей соответствует коду Грея для разбиений на части, не превосходящие m. Мы будем работать именно с этим последним ограничением.

Общее количество кодов Грея для разбиений очень велико: для $n = 7$ их 52, для $n = 8$ — 652, для $n = 9$ — 298 896, для $n = 10$ — 2 291 100 484. Однако реально простое построение их неизвестно. Вероятно, причина в том, что лишь некоторые разбиения имеют только двух соседей, а именно разбиения $d^{n/d}$ при $1 < d < n$ и n, кратном d. У таких разбиений предшествующими и последующими должны быть разбиения $\left\{(d+1)\, d^{n/d-2}\, (d-1)\,, d^{n/d-1}\, (d-1)\, 1\right\}$, и это требование, похоже, исключает любой простой рекурсивный подход.

Карла Сэведж (Carla Savage) [*J. Algorithms*, **10** (1989), 577–595] нашла способ преодоления этих трудностей ценой всего лишь небольшой сложности. Пусть

$$\mu\,(m,n) = \overbrace{m\; m\; \ldots\; m}^{\lfloor n/m \rfloor}\ (n \bmod m) \tag{60}$$

представляет собой лексикографически наибольшее разбиение n с частями, не превышающими m. Наша цель состоит в построении рекурсивно определенных путей Грея $L\,(m,n)$ и $M\,(m,n)$ от разбиения 1^n до $\mu\,(m,n)$, где $L\,(m,n)$ проходит по всем разбиениям, части которых ограничены m, в то время как $M\,(m,n)$ пробегает не только по этим разбиениям, но и включает разбиения, наибольшая часть которых равна $m+1$, при условии, что все прочие части строго меньше m. Например, $L\,(3,8)$ — 11111111, 2111111, 311111, 221111, 22211, 2222, 3221, 32111, 3311, 332, в то время как $M\,(3,8)$ —

$$\begin{gathered} 11111111, 2111111, 221111, 22211, 2222, 3221, \\ 3311, 32111, 311111, 41111, 4211, 422, 332; \end{gathered} \tag{61}$$

дополнительные разбиения, начинающиеся с 4, дают нам "пространство подгонки" (wiggle room) в других частях рекурсии. Мы определим $L\,(m,n)$ для всех $n \geqslant 0$, а $M\,(m,n)$ — только для $n > 2m$.

Почти работоспособна следующая конструкция, проиллюстрированная для упрощения при $m = 5$:

$$L\,(5) = \left\{\begin{array}{l} L\,(3) \\ 4\,L\,(\infty)^R \\ 5\,L\,(\infty) \end{array}\right\} \text{ при } n \leqslant 7; \quad \left\{\begin{array}{l} L\,(3) \\ 4\,L\,(2)^R \\ 5\,L\,(2) \\ 4\,3\,1 \\ 4\,4 \\ 5\,3 \end{array}\right\} \text{ при } n = 8; \quad \left\{\begin{array}{l} M\,(4) \\ 5\,4\,L\,(4)^R \\ 5\,5\,L\,(5) \end{array}\right\} \text{ при } n \geqslant 9; \tag{62}$$

$$M\,(5) = \left\{\begin{array}{l} L\,(4) \\ 5\,L\,(4)^R \\ 6\,L\,(3) \\ 6\,4\,L\,(\infty)^R \\ 5\,5\,L\,(\infty) \end{array}\right\} \text{ при } 11 \leqslant n \leqslant 13; \quad \left\{\begin{array}{l} L\,(4) \\ 5\,M\,(4)^R \\ 6\,L\,(4) \\ 5\,5\,4\,L\,(4)^R \\ 5\,5\,5\,L\,(5) \end{array}\right\} \text{ при } n \geqslant 14. \tag{63}$$

Здесь параметр n в $L\,(m,n)$ и $M\,(m,n)$ опущен, поскольку может быть выведен из контекста; предполагается, что каждые L и M генерируют разбиения для любого количества, остающегося после вычитания предыдущих частей. Так, например, (63) указывает, что

$$M\,(5,14) = L\,(4,14)\,,\ 5M\,(4,9)^R\,,\ 6L\,(4,8)\,,\ 5\,5\,4L\,(4,0)^R\,,\ 5\,5\,5L\,(5,-1)\,;$$

последовательность $L\,(5,-1)$ в действительности пустая, а $L\,(4,0)$ представляет собой пустую строку, так что последняя часть $M\,(5,14)$ равна $5\,5\,4 = \mu\,(5,14)$, как и должно быть. Запись $L\,(\infty)$ означает $L\,(\infty,n) = L\,(n,n)$, путь Грея всех разбиений n, начинающихся с 1^n и заканчивающихся n^1.

В общем случае $L\,(m)$ и $M\,(m)$ определяются для всех $m \geqslant 3$, по сути, одними и теми же правилами, если цифры 2, 3, 4, 5 и 6 в (62) и (63) заменить соответственно на $m-3$, $m-2$, $m-1$, m и $m+1$. Диапазоны $n \leqslant 7$, $n = 8$ и $n \geqslant 9$ превращаются в $n \leqslant 2m-3$, $n = 2m-2$, $n \geqslant 2m-1$; диапазоны $11 \leqslant n \leqslant 13$ и $n \geqslant 14$ становятся диапазонами $2m+1 \leqslant n \leqslant 3m-2$ и $n \geqslant 3m-1$. Последовательности $L\,(0)$, $L\,(1)$, $L\,(2)$ имеют очевидные определения, поскольку эти пути единственны при $m \leqslant 2$. Последовательность $M\,(2)$ представляет собой $1^n, 21^{n-2}, 31^{n-3}, 221^{n-4}, 2221^{n-6}, \ldots, \mu\,(2,n)$ при $n \geqslant 5$.

Теорема S. *Пути Грея $L'\,(m,n)$ для $m,n \geqslant 0$ и $M'\,(m,n)$ для $n \geqslant 2m+1 \geqslant 5$ существуют для всех разбиений с описанными выше свойствами, за исключением случая $L'\,(4,6)$. Кроме того, L' и M' удовлетворяют взаимным рекурсиям (62) и (63), за исключением нескольких случаев.*

Доказательство. Выше мы отмечали, что (62) и (63) *почти* работоспособны; читатель может убедиться, что затруднения возникают только в случае $L\,(4,6)$, когда (62) дает

$$L\,(4,6) = L\,(2,6)\,,\ 3L\,(1,3)^R\,,\ 4L\,(1,2)\,,\ 321,\ 33,\ 42 = \\ = 111111,\ 21111,\ 2211,\ 222,\ 3111,\ 411,\ 321,\ 33,\ 42. \tag{64}$$

Если $m > 4$, все в порядке, поскольку переход от конца $L\,(m-2, 2m-2)$ к началу $(m-1)\,L\,(m-3, m-1)^R$ является переходом от $(m-2)\,(m-2)\,2$ к $(m-1)\,(m-3)\,2$. Удовлетворительного пути $L\,(4,6)$ не существует, поскольку все коды Грея через эти девять разбиений должны заканчиваться одним из следующих разбиений: 411, 33, 3111, 222, 2211.

Для того чтобы нейтрализовать эту аномалию, необходимо исправить определения $L\,(m,n)$ и $M\,(m,n)$ в восьми местах, где вызывается "некорректная подпрограмма" $L\,(4,6)$. Один из простых путей состоит в следующих определениях:

$$L'\,(4,6) = 111111,\ 21111,\ 3111,\ 411,\ 321,\ 33,\ 42; \\ L'\,(3,5) = 11111,\ 2111,\ 221,\ 311,\ 32. \tag{65}$$

Таким образом, мы опускаем в $L\,(4,6)$ 222 и 2211; мы также перепрограммируем $L\,(3,5)$ так, чтобы 2111 было по соседству с 221. В этом случае, как демонстрирует упражнение 60, всегда легко "состыковать" два разбиения, отсутствующие в $L\,(4,6)$. ▮

Упражнения

► **1.** [*M21*] Найдите формулу для общего количества размещений в каждой из задач двенадцатизадачия. Например, количество n-кортежей из m вещей равно m^n. (Воспользуйтесь обозначением из (38) там, где это можно, и будьте аккуратны, чтобы ваши формулы выполнялись даже при значениях $m = 0$ или $n = 0$.)

► **2.** [*20*] Покажите, что небольшое изменение шага H1 дает алгоритм, который генерирует все разбиения n *не более чем* на m частей.

3. [*M17*] Разбиение $a_1 + \cdots + a_m$ числа n на m частей $a_1 \geqslant \ldots \geqslant a_m$ *оптимально сбалансировано*, если $|a_i - a_j| \leqslant 1$ для $1 \leqslant i, j \leqslant m$. Докажите, что имеется ровно одно такое разбиение, какими бы ни были $n \geqslant m \geqslant 1$, и приведите простую формулу, выражающую j-ю часть a_j как функцию от j, m и n.

4. [*M22*] (Гидеон Эрлих (Gideon Ehrlich), 1974.) Каково лексикографически наименьшее разбиение n, в котором все части $\geqslant r$? Например, при $n = 19$ и $r = 5$ ответ — 766.

► **5.** [*23*] Разработайте алгоритм, который генерирует все разбиения n в виде количества частей $c_1 \ldots c_n$ из (8). Сгенерируйте их в солексном порядке, т.е. лексикографическом порядке $c_n \ldots c_1$, который эквивалентен лексикографическому порядку соответствующих разбиений $a_1 a_2 \ldots$. Для эффективности поддерживайте таблицу связей $l_0 l_1 \ldots l_n$, такую, что если различные значения k, для которых $c_k > 0$, представляют собой $k_1 < \cdots < k_t$, то

$$l_0 = k_1, \quad l_{k_1} = k_2, \quad \ldots, \quad l_{k_{t-1}} = k_t, \quad l_{k_t} = 0.$$

(Так, разбиение 331 будет представлено как $c_1 \ldots c_7 = 1020000$, $l_0 = 1$, $l_1 = 3$ и $l_3 = 0$; прочие связи l_2, l_4, l_5, l_6, l_7 могут принимать любые значения.)

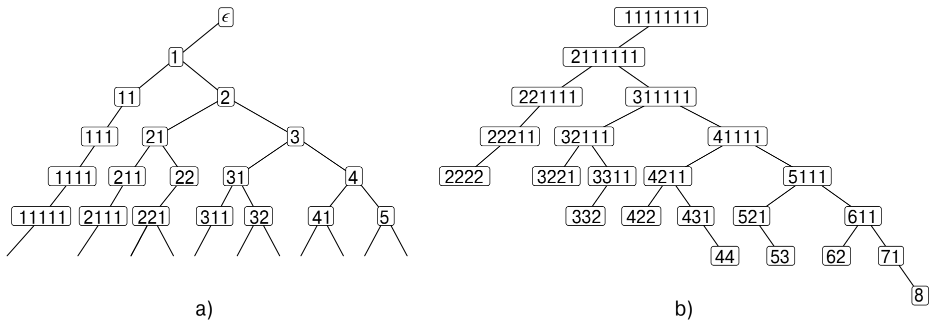
6. [*20*] Разработайте алгоритм для вычисления $b_1b_2\ldots = (a_1a_2\ldots)^T$ для заданного $a_1a_2\ldots$.

7. [*M20*] Предположим, что $a_1\ldots a_n$ и $a'_1\ldots a'_n$ — разбиения n, такие, что $a_1 \geqslant \cdots \geqslant a_n \geqslant 0$ и $a'_1 \geqslant \cdots \geqslant a'_n \geqslant 0$, и пусть им соответствуют сопряженные разбиения $b_1\ldots b_n = (a_1\ldots a_n)^T$ и $b'_1\ldots b'_n = (a'_1\ldots a'_n)^T$. Покажите, что $b_1\ldots b_n < b'_1\ldots b'_n$ тогда и только тогда, когда $a_n\ldots a_1 < a'_n\ldots a'_1$.

8. [*15*] Пусть $(p_1\ldots p_t, q_1\ldots q_t)$ — краевое представление разбиения $a_1a_2\ldots$, как приведено в (15) и (16). Какой вид в этом случае имеет сопряженное разбиение $(a_1a_2\ldots)^T = b_1b_2\ldots$?

9. [*22*] Пусть $a_1a_2\ldots a_m$ и $b_1b_2\ldots b_m = (a_1a_2\ldots a_m)^T$ — сопряженные разбиения. Покажите, что мультимножества $\{a_1+1, a_2+2, \ldots, a_m+m\}$ и $\{b_1+1, b_2+2, \ldots, b_m+m\}$ равны.

10. [*21*] При рассмотрении разбиений зачастую полезными оказываются бинарные деревья двух простых видов: *a*) дерево, которое включает все разбиения всех целых чисел; *b*) дерево, которое включает все разбиения данного целого n (на рисунке показано дерево для $n = 8$).



a) b)

Выведите общее правило, лежащее в основе этих конструкций. Какой порядок обхода дерева соответствует лексикографическому порядку разбиений?

11. [*M22*] Сколько имеется способов заплатить один евро монетами достоинством 1, 2, 5, 10, 20, 50 и/или 100 центов? А если можно использовать не больше двух монет каждого достоинства?

▶ **12.** [*M21*] (Л. Эйлер (L. Euler), 1750.) Воспользуйтесь производящей функцией для доказательства того, что количество способов разбиения n на *различные* части равно количеству способов разбиения n на *нечетные* части. Например, $5 = 4+1 = 3+2$; $5 = 3+1+1 = 1+1+1+1+1$.

Примечание: два следующих упражнения используют комбинаторные методы для доказательства расширений этой знаменитой теоремы.

▶ **13.** [*M22*] (Ф. Франклин (F. Franklin), 1882.) Найдите взаимно однозначное соответствие между разбиениями n, которые имеют ровно k четных частей, и разбиениями n, в которых можно сформировать k пар равных частей. (Например, в разбиении 8666433211111 имеются пары 66, 33, 11 и 11, так что $k = 4$. Случай $k = 0$ соответствует результату, полученному Эйлером.)

14. [*M28*] (Д.Д. Сильвестер (J.J. Sylvester), 1882.) Найдите взаимно однозначное соответствие между разбиениями n на различные части $a_1 > a_2 > \cdots > a_m$, в которых имеется ровно k "просветов" $a_j > a_{j+1} + 1$, и разбиениями n на нечетные части с $k+1$ разными значениями. (Например, при $k = 0$ это построение доказывает, что количество способов записать n как сумму последовательных целых чисел равно количеству четных делителей n.)

15. [*M20*] (Д.Д. Сильвестер (J.J. Sylvester).) Найдите производящую функцию для количества разбиений, являющихся *самосопряженными* (т.е. таких, что $\alpha = \alpha^T$).

16. [*M21*] Найдите производящую функцию для разбиений следа k и просуммируйте ее по k для получения нетривиального тождества.

17. [*M26*] *Объединенным разбиением* (joint partition) n называется пара последовательностей $(a_1, \ldots, a_r;\ b_1, \ldots, b_s)$ положительных целых чисел, у которых

$$a_1 \geqslant \cdots \geqslant a_r, \quad b_1 > \cdots > b_s \quad \text{и} \quad a_1 + \cdots + a_r + b_1 + \cdots + b_s = n.$$

Таким образом, при $s = 0$ мы получаем обычное разбиение, а при $r = 0$ — разбиение на различные части.

a) Найдите простую формулу для производящей функции $\sum u^{r+s} v^s z^n$, где суммирование выполняется по всем объединенным разбиениям n с r обычных частей a_i и s различных частей b_j.

b) Аналогично, найдите простую формулу для $\sum v^s z^n$, где суммирование выполняется по всем объединенным разбиениям, которые состоят ровно из $r + s = t$ частей, для заданного значения t.

c) Какое тождество вы вывели?

► **18.** [*M23*] (Дорон Зайльбергер (Doron Zeilberger).) Покажите, что существует взаимно однозначное соответствие между парами последовательностей целых чисел $(a_1, a_2, \ldots, a_r;\ b_1, b_2, \ldots, b_s)$, таких, что

$$a_1 \geqslant a_2 \geqslant \cdots \geqslant a_r, \quad b_1 > b_2 > \cdots > b_s,$$

и парами последовательностей целых чисел $(c_1, c_2, \ldots, c_{r+s};\ d_1, d_2, \ldots, d_{r+s})$, таких, что

$$c_1 \geqslant c_2 \geqslant \cdots \geqslant c_{r+s}, \quad d_j \in \{0,1\} \quad \text{для } 1 \leqslant j \leqslant r+s,$$

связанных уравнениями для мультимножеств

$$\{a_1, a_2, \ldots, a_r\} = \{c_j | d_j = 0\} \quad \text{и} \quad \{b_1, b_2, \ldots, b_s\} = \{c_j + r + s - j | d_j = 1\}.$$

В результате получаем интересное тождество

$$\sum_{\substack{a_1 \geqslant a_2 \geqslant \cdots \geqslant a_r \\ b_1 > \cdots > b_s > 0}} u^{r+s} v^s z^{a_1 + \cdots + a_r + b_1 + \cdots + b_s} =$$

$$= \sum_{\substack{c_1 \geqslant \cdots \geqslant c_t > 0 \\ d_1, \ldots, d_t \in \{0,1\}}} u^t v^{d_1 + \cdots + d_t} z^{c_1 + \cdots + c_t + (t-1)d_1 + \cdots + d_{t-1}}.$$

19. [*M21*] (Э. Гейне (E. Heine), 1847.) Докажите четырехпараметрическое тождество

$$\prod_{m=1}^{\infty}\frac{(1-wxz^m)\,(1-wyz^m)}{(1-wz^m)\,(1-wxyz^m)}=$$
$$=\sum_{k=0}^{\infty}\frac{w^k\,(x-1)\,(z-1)\cdots\left(x-z^{k-1}\right)(y-1)\,(y-z)\cdots\left(y-z^{k-1}\right)z^k}{(1-z)\,(1-z^2)\cdots(1-z^k)\,(1-wz)\,(1-wz^2)\cdots(1-wz^k)}.$$

Указание: выполните суммирование по k или l в формуле

$$\sum_{k,l\geqslant 0}u^kv^lz^{kl}\frac{(z-az)\left(z-az^2\right)\cdots\left(z-az^k\right)}{(1-z)\,(1-z^2)\cdots(1-z^k)}\frac{(z-bz)\left(z-bz^2\right)\cdots\left(z-bz^l\right)}{(1-z)\,(1-z^2)\cdots(1-z^l)}$$

и рассмотрите упрощение, возникающее при $b=auz$.

► **20.** [*M21*] Сколько приблизительно времени займет вычисление таблицы разбиений чисел $p\,(n)$ для $1\leqslant n\leqslant N$ с использованием рекуррентного соотношения Эйлера (20)?

21. [*M21*] (Л. Эйлер (L. Euler).) Пусть $q\,(n)$ — количество разбиений на различные части. Как лучше вычислить $q\,(n)$, зная значения $p\,(1),\ \ldots,\ p\,(n)$?

22. [*HM21*] (Л. Эйлер (L. Euler).) Пусть $\sigma\,(n)$ — сумма всех положительных делителей положительного целого числа n. Тогда $\sigma\,(n)=n+1$ для простого n и может оказаться существенно больше n для “высокосоставного” n. Докажите, что, несмотря на достаточно хаотичное поведение, $\sigma\,(n)$ удовлетворяет почти такому же рекуррентному соотношению (20), что и количество разбиений:

$$\sigma\,(n)=\sigma\,(n-1)+\sigma\,(n-2)-\sigma\,(n-5)-\sigma\,(n-7)+\sigma\,(n-12)+\sigma\,(n-15)-\cdots$$

для $n\geqslant 1$, с тем отличием, что, если в правой части встречается член ‘$\sigma\,(0)$’, вместо него используется значение ‘n’. Например, $\sigma\,(11)=1+11=\sigma\,(10)+\sigma\,(9)-\sigma\,(6)-\sigma\,(4)=18+13-12-7$; $\sigma\,(12)=1+2+3+4+6+12=\sigma\,(11)+\sigma\,(10)-\sigma\,(7)-\sigma\,(5)+12=12+18-8-6+12$.

23. [*HM25*] Используйте тождество Якоби (19) для доказательства еще одной открытой им формулы:

$$\prod_{k=1}^{\infty}\left(1-z^k\right)^3=1-3z+5z^3-7z^6+9z^{10}-\cdots=\sum_{n=0}^{\infty}(-1)^n\,(2n+1)\,z^{\binom{n+1}{2}}.$$

24. [*M26*] (С. Рамануджан (S. Ramanujan), 1919.) Пусть $A\,(z)=\prod_{k=1}^{\infty}\left(1-z^k\right)^4$.

a) Докажите, что $[z^n]\,A\,(z)$ кратно 5, если $n \bmod 5=4$.

b) Докажите, что тем же свойством обладает $[z^n]\,A\,(z)\,B\,(z)^5$, где B — произвольный степенной ряд с целыми коэффициентами.

c) Следовательно, $p\,(n)$ кратно пяти, если $n \bmod 5=4$.

25. [*HM27*] Улучшите оценку $\ln P\,(e^{-t})$ (22) при помощи (a) формулы суммирования Эйлера и (b) преобразования Меллина. *Указание*: дилогарифмическая функция $\mathrm{Li}_2\,(x) = x/1^2 + x^2/2^2 + x^3/3^2 + \cdots$ удовлетворяет соотношению $\mathrm{Li}_2\,(x) + \mathrm{Li}_2\,(1-x) = \zeta\,(2) - (\ln x)\ln\,(1-x)$.

26. [*NM22*] В упражнении 5.2.2–44 и 5.2.2–51 мы рассмотрели два способа доказательства того, что

$$\sum_{k=1}^{\infty} e^{-k^2/n} = \frac{1}{2}\left(\sqrt{\pi n} - 1\right) + O\left(n^{-M}\right) \text{ для всех } M > 0.$$

Покажите, что формула суммирования Пуассона дает более строгий результат.

27. [*HM23*] Вычислите (29) и завершите вычисления, приводящие к теореме D.

28. [*HM42*] (Д.Г. Лемер (D.H. Lehmer).) Покажите, что коэффициенты Харди–Рамануджана–Радемахера $A_k\,(n)$, определенные в (34), обладают следующими замечательными свойствами:

a) если k нечетно, то $A_{2k}\left(km + 4n + \left(k^2-1\right)/8\right) = A_2\,(m)\,A_k\,(n)$;

b) если p — простое, $p^e > 2$ и $k \perp 2p$, то

$$A_{p^e k}\left(k^2 m + p^{2e} n - \left(k^2 + p^{2e} - 1\right)/24\right) = (-1)^{[p^e=4]} A_{p^e}\,(m)\,A_k\,(n)\,;$$

c) в этой формуле $k^2 + p^{2e} - 1$ кратно 24, если p или k делятся на 2 или 3; в противном случае деление на 24 должно выполняться по модулю $p^e k$;

d) если p — простое, $|A_{p^e}\,(n)| < 2^{[p>2]} p^{e/2}$;

e) если p — простое, $A_{p^e}\,(n) \neq 0$ тогда и только тогда, когда $1 - 24n$ — квадратичный вычет по модулю p и либо $e = 1$, либо $24n \bmod p \neq 1$;

f) вероятность того, что $A_k\,(n) = 0$, если k делится ровно на t простых чисел, не меньших 5, а n — случайное число, приблизительно равна $1 - 2^{-t}$.

► **29.** [*M16*] Обобщая (41), вычислите сумму $\sum_{a_1 \geqslant a_2 \geqslant \cdots \geqslant a_m \geqslant 1} z_1^{a_1} z_2^{a_2} \cdots z_m^{a_m}$.

30. [*M17*] Найдите формулы для сумм

$$\text{(a)}\ \sum_{k\geqslant 0} \left|\begin{matrix} n - km \\ m - 1 \end{matrix}\right|; \qquad \text{(b)}\ \sum_{k\geqslant 0} \left|\begin{matrix} n \\ m - k \end{matrix}\right|.$$

(Эти суммы конечны, поскольку при больших k суммируемые члены равны 0.)

31. [*M24*] (А. де Морган (A. De Morgan), 1843.) Покажите, что $\left|{n \atop 2}\right| = \lfloor n/2 \rfloor$ и $\left|{n \atop 3}\right| = \left\lfloor \left(n^2+6\right)/12 \right\rfloor$; найдите аналогичную формулу для $\left|{n \atop 4}\right|$.

32. [*M15*] Докажите, что $\left|{n \atop m}\right| \leqslant p\,(n-m)$ для всех $m, n \geqslant 0$. В каком случае неравенство превращается в равенство?

33. [*HM20*] Воспользуйтесь тем фактом, что имеется ровно $\binom{n-1}{m-1}$ ***композиций*** n из m частей (см. определение композиции в 7.2.1.3–(9)), для доказательства нижней границы $\left|{n \atop m}\right|$. Затем установите $m = \lfloor\sqrt{n}\rfloor$ для получения элементарной нижней границы $p\,(n)$.

► **34.** [*HM21*] Покажите, что $\left|{n-m(m-1)/2 \atop m}\right|$ — количество разбиений n на m различных частей. Таким образом,

$$\left|{n \atop m}\right| = \frac{n^{m-1}}{m!\,(m-1)!}\left(1 + O\left(\frac{m^3}{n}\right)\right) \quad \text{при } m \leqslant n^{1/3}.$$

35. [*HM21*] Рассмотрим распределение вероятностей Эрдеша–Ленера (43).

a) Какое значение x наиболее вероятно?

b) Какое значение x является медианой?

c) Какое значение x является средним значением?

d) Чему равно стандартное отклонение?

36. [*HM24*] Докажите ключевую оценку (47), необходимую для теоремы E.

37. [*M22*] Докажите лемму (48) о том, что при использовании принципа включения-исключения частичные суммы "берут в вилку" истинное значение, проанализировав, сколько раз разбиение ровно с q различными частями, превосходящими m, учитывается в r-й частичной сумме.

38. [*M20*] Какова производящая функция для разбиений n ровно на m частей с наибольшей частью l?

► **39.** [*M*25] (Ф. Франклин (F. Franklin).) Обобщая теорему C, покажите, что при $0 \leqslant k \leqslant m$

$$[z^n]\,\frac{(1-z^{l+1})\ldots(1-z^{l+k})}{(1-z)\,(1-z^2)\ldots(1-z^m)}$$

представляет собой количество разбиений $a_1 a_2 \ldots$ числа n на m или меньшее количество частей, обладающих тем свойством, что $a_1 \leqslant a_{k+1} + l$.

40. [*M22*] (А. Коши (A. Cauchy).) Что представляет собой производящая функция для разбиений на m частей, где все части *различны* и меньше l?

41. [*HM42*] Расширьте формулу Харди–Рамануджана–Радемахера (32) для получения сходящегося ряда для разбиений n не более чем на m частей, ни одна из которых не превосходит l.

42. [*HM42*] Найдите ограничивающую область, аналогичную (49), для случайных разбиений n не более чем на $\theta\sqrt{n}$ частей, причем части не превосходят $\varphi\sqrt{n}$, в предположении, что $\theta\varphi > 1$.

43. [*M21*] Сколько для заданных n и k имеется разбиений числа n, таких, что $a_1 > a_2 > \cdots > a_k$?

► **44.** [$M22$] У какого количества разбиений числа n две наименьшие части равны?

45. [*HM21*] Вычислите асимптотическое значение $p(n-1)/p(n)$ с относительной ошибкой $O\left(n^{-2}\right)$.

46. [*M20*] Что больше — $T_2'(n)$ или $T_2''(n)$ — в тексте анализа алгоритма P?

► **47.** [*HM22*] (А. Ньенхуис (A. Nijenhuis) и Г.С. Вильф (H.S. Wilf), 1975.) Приведенный далее простой алгоритм, основываясь на таблице количеств разбиений $p(0), p(1), \ldots, p(n)$, генерирует случайное разбиение числа n с использованием представления в виде количества частей (8). Докажите, что он генерирует все разбиения с одинаковой вероятностью.

N1. [Инициализация.] Установить $m \leftarrow n$ и $c_1 \ldots c_n \leftarrow 0 \ldots 0$.

N2. [Выполнено?] Завершить работу, если $m = 0$.

N3. [Генерация.] Сгенерировать случайное целое число M в диапазоне $0 \leqslant M < mp(m)$.

N4. [Выбор частей.] Установить $s \leftarrow 0$. Затем для $j = 1, 2, \ldots, n$ и для $k = 1, 2, \ldots, \lfloor m/j \rfloor$ многократно устанавливать $s \leftarrow s + kp(m - jk)$ до тех пор, пока не будет выполнено условие $s > M$.

N5. [Обновление.] Установить $c_k \leftarrow c_k + j$, $m \leftarrow m - jk$ и вернуться к шагу N2. ▮

Указание: на шаге N4, основанном на тождестве

$$\sum_{j=1}^{m} \sum_{k=1}^{\lfloor m/j \rfloor} kp(m - jk) = mp(m),$$

выбирается пара значений(j, k) с вероятностью $kp(m - jk)/(mp(m))$.

48. [*HM40*] Проанализируйте время работы алгоритма из предыдущего упражнения.

► **49.** [*HM26*]

a) Какой вид имеет производящая функция $F(z)$ для суммы наименьших частей всех разбиений n? (Ряд начинается с $z + 3z^2 + 5z^3 + 9z^4 + 12z^5 + \cdots$.)

b) Найдите асимптотическое значение $[z^n] F(z)$ с относительной ошибкой $O\left(n^{-1}\right)$.

50. [*HM33*] Обозначим в рекуррентных соотношениях (56) и (57) $c(m) = c_m(2m)$.

a) Докажите, что $c_m(m + k) = m - k + c(k)$ для $0 \leqslant k \leqslant m$.

b) Следовательно, (58) выполняется для $m \leqslant n \leqslant 2m$, если $c(m) < 3p(m)$ для всех m.

c) Покажите, что $c(m) - m$ равно сумме вторых наименьших частей всех разбиений m.

d) Найдите взаимно однозначное соответствие между всеми разбиениями n, у которых вторая наименьшая часть равна k, и всеми разбиениями чисел, не превышающих n, у которых наименьшая часть равна $k+1$.

e) Опишите производящую функцию $\sum_{m\geqslant 0} c\,(m)\,z^m$.

f) Сделайте вывод, что $c\,(m) < 3p\,(m)$ для всех $m \geqslant 0$.

51. [*M46*] Выполните детальный анализ алгоритма H.

► **52.** [*M21*] Какой вид имеет миллионное разбиение, сгенерированное алгоритмом P для $n = 64$? *Указание*: $p\,(64) = 1\,741\,630 = 1\,000\,000 + \left|{77 \atop 13}\right| + \left|{60 \atop 10}\right| + \left|{47 \atop 8}\right| + \left|{35 \atop 5}\right| + \left|{27 \atop 3}\right| + \left|{22 \atop 2}\right| + \left|{18 \atop 1}\right| + \left|{15 \atop 0}\right|$.

► **53.** [*M21*] Какой вид имеет миллионное разбиение, сгенерированное алгоритмом H для $m = 32$ и $n = 100$? *Указание*: $999\,999 = \left|{80 \atop 12}\right| + \left|{66 \atop 11}\right| + \left|{50 \atop 7}\right| + \left|{41 \atop 6}\right| + \left|{33 \atop 5}\right| + \left|{26 \atop 4}\right| + \left|{21 \atop 4}\right|$.

► **54.** [*M30*] Разбиение $\alpha = a_1a_2\ldots$ *мажоризирует* (majorize) разбиение $\beta = b_1b_2\ldots$, что записывается как $\alpha \succcurlyeq \beta$ или $\beta \preccurlyeq \alpha$, если $a_1 + \cdots + a_k \geqslant b_1 + \cdots + b_k$ для всех $k \geqslant 0$.

a) Истинно или ложно утверждение: из $\alpha \succcurlyeq \beta$ вытекает $\alpha \geqslant \beta$ (лексикографически)?

b) Истинно или ложно утверждение: из $\alpha \succcurlyeq \beta$ вытекает $\beta^T \succcurlyeq \alpha^T$?

c) Покажите, что два любых разбиения n имеют наибольшую нижнюю границу $\alpha\wedge\beta$, такую, что $\alpha \succcurlyeq \gamma$ и $\beta \succcurlyeq \gamma$ тогда и только тогда, когда $\alpha\wedge\beta \succcurlyeq \gamma$. Поясните, как можно вычислить $\alpha \wedge \beta$.

d) Аналогично, поясните, как вычислить наименьшую верхнюю границу $\alpha \vee \beta$, такую, что $\gamma \succcurlyeq \alpha$ и $\gamma \succcurlyeq \beta$ тогда и только тогда, когда $\gamma \succcurlyeq \alpha \vee \beta$.

e) Если α имеет l частей, а β имеет m частей, то сколько частей имеют $\alpha \wedge \beta$ и $\alpha \vee \beta$?

f) Истинно или ложно утверждение: если α состоит из различных частей и β состоит из различных частей, то же самое можно сказать и об $\alpha \wedge \beta$ и $\alpha \vee \beta$.

► **55.** [*M37*] Продолжая выполнение предыдущего упражнения, назовем α ***покрытием*** (cover) β, если $\alpha \succcurlyeq \beta$, $\alpha \neq \beta$ и из $\alpha \succcurlyeq \gamma \succcurlyeq \beta$ следует $\gamma = \alpha$ или $\gamma = \beta$. Например, на рис. 32 показано отношение покрытия между разбиениями числа 12.

a) Будем записывать $\alpha \vdash \beta$, если $\alpha = a_1a_2\ldots$ и $\beta = b_1b_2\ldots$ представляют собой разбиения, для которых $b_k = a_k - [k = l] + [k = l+1]$ для всех $k \geqslant 1$ и некоторого $l \geqslant 1$. Докажите, что α покрывает β тогда и только тогда, когда $\alpha \vdash \beta$ или $\beta^T \vdash \alpha^T$.

b) Покажите, что есть простой способ выяснить, верно ли, что α покрывает β, путем рассмотрения краевого представления α и β.

c) Пусть $n = \binom{n_2}{2} + \binom{n_1}{1}$, где $n_2 > n_1 \geqslant 0$. Покажите, что ни одно разбиение n не покрывает больше $n_2 - 2$ разбиений.

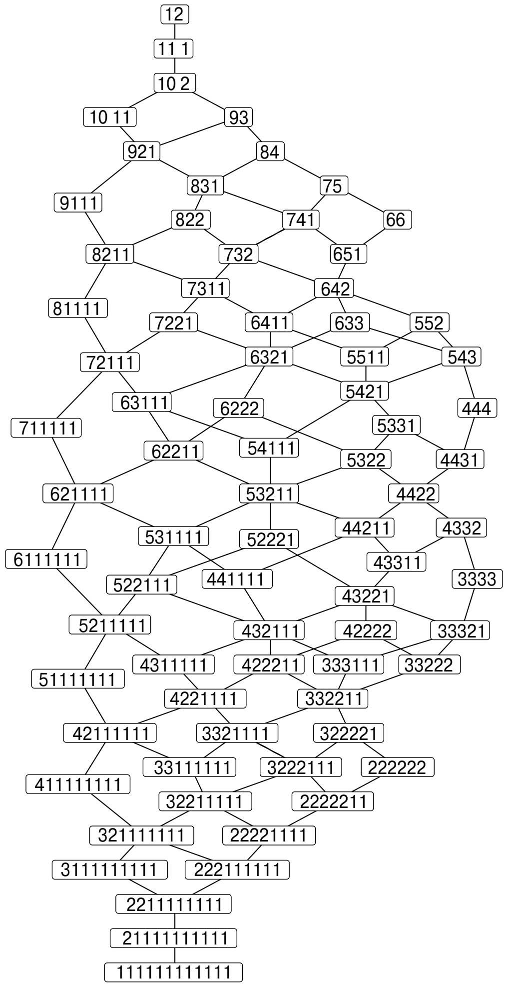


Рис. 32. Решетка мажоризации для разбиений 12 (см. упражнения 54–58)

d) Будем называть разбиение μ *минимальным*, если не существует разбиения λ, такого, что $\mu \succ \lambda$. Докажите, что μ минимально тогда и только тогда, когда μ^T имеет различные части.

e) Предположим, что $\alpha = \alpha_0 \succ \alpha_1 \succ \cdots \succ \alpha_k$ и $\alpha = \alpha'_0 \succ \alpha'_1 \succ \cdots \succ \alpha'_{k'}$, где α_k и $\alpha'_{k'}$ — минимальные разбиения. Докажите, что $k = k'$ и $\alpha_k = \alpha'_{k'}$.

f) Поясните, как вычислить лексикографически наименьшее разбиение на различные части, которое мажоризирует данное разбиение α.

g) Опишите лексикографически наименьшее разбиение λ_n числа n на различные части. Чему равна длина всех путей $n^1 = \alpha_0 \succ \alpha_1 \succ \cdots \succ \lambda_n^T$?

h) Чему равна длина длиннейшего и кратчайшего путей вида $n^1 = \alpha_0, \alpha_1, \ldots, \alpha_l = 1^n$, где α_j покрывает α_{j+1} для всех $0 \leqslant j < l$?

► **56.** [*M27*] Разработайте алгоритм для генерации всех разбиений α, таких, что $\lambda \preccurlyeq \alpha \preccurlyeq \mu$, для данных разбиений λ и μ, $\lambda \preccurlyeq \mu$.

Примечание. Такой алгоритм имеет множество применений. Например, для генерации всех разбиений, которые имеют m частей, причем ни одна из частей не превосходит l, мы можем положить λ минимальным разбиением такого вида, т.е., как в упражнении 3, $\lceil n/m \rceil \ldots \lfloor n/m \rfloor$, а μ — наибольшим, т.е. $\bigl((n-m+1)\,1^{m-1}\bigr) \wedge \bigl(l^{\lfloor n/l \rfloor}\,(n \bmod l)\bigr)$. Аналогично, согласно известной теореме Х.Г. Ландау (H.G. Landau) [*Bull. Math. Biophysics*, **15** (1953), 143–148], разбиения $\binom{m}{2}$, такие, что

$$\left\lfloor \frac{m}{2} \right\rfloor^{\lfloor m/2 \rfloor} \left\lfloor \frac{m-1}{2} \right\rfloor^{\lceil m/2 \rceil} \preccurlyeq \alpha \preccurlyeq (m-1)\,(m-2)\ldots 21,$$

представляют собой “векторы счетов” в круговом турнире, т.е. разбиения $a_1 \ldots a_m$, когда игрок на j-м месте побеждает в a_j играх.

57. [*M22*] Предположим, что матрица (a_{ij}) из нулей и единиц имеет суммы элементов строк $r_i = \sum_j a_{ij}$ и суммы элементов столбцов $c_j = \sum_i a_{ij}$. Тогда $\lambda = r_1 r_2 \ldots$ и $\mu = c_1 c_2 \ldots$ — разбиения $n = \sum_{i,j} a_{ij}$. Докажите, что такая матрица существует тогда и только тогда, когда $\lambda \preccurlyeq \mu^T$.

58. [*M23*] (*Симметричные средние.*) Пусть $\alpha = a_1 \ldots a_m$ и $\beta = b_1 \ldots b_m$ — разбиения n. Докажите, что неравенство

$$\frac{1}{m!} \sum x_{p_1}^{a_1} \ldots x_{p_m}^{a_m} \geqslant \frac{1}{m!} \sum x_{p_1}^{b_1} \ldots x_{p_m}^{b_m}$$

выполняется для любых неотрицательных значений переменных $(x_1, \ldots, x_m)$, где сумма берется по всем $m!$ перестановкам $\{1, \ldots, m\}$, тогда и только тогда, когда $\alpha \succcurlyeq \beta$. (Например, это неравенство сводится к $(y_1 + \cdots + y_n)/n \geqslant (y_1 \ldots y_n)^{1/n}$ в частном случае $m = n$, $\alpha = n0\ldots0$, $\beta = 11\ldots1$, $x_j = y_j^{1/n}$.)

59. [*M22*] Путь Грея (59) симметричен в том смысле, что обращенная последовательность $6, 51, \ldots, 111111$ имеет тот же вид, что и сопряженная последовательность $(111111)^T$, $(21111)^T$, $\ldots$, $(6)^T$. Найдите все пути Грея $\alpha_1, \ldots, \alpha_{p(n)}$, симметричные в данном смысле.

60. [*23*] Завершите доказательство теоремы S, изменяя определения $L(m,n)$ и $M(m,n)$ во всех местах, где в (62) и (63) вызывается $L(4,6)$.

61. [*26*] Реализуйте схему генерации разбиений на основе теоремы S, всегда указывающей две части, которые должны измениться между посещениями.

62. [*46*] Докажите или опровергните следующее утверждение: для всех достаточно больших целых чисел n и $3 \leqslant m < n$, таких, что $n \bmod m \neq 0$, и для всех разбиений α числа n, у которых $a_1 \leqslant m$, существует путь Грея для всех разбиений с частями, не превышающими m, начинающийся с 1^n и заканчивающийся α, за исключением $\alpha = 1^n$ и $\alpha = 21^{n-2}$.

63. [*47*] Для каких разбиений λ и μ имеется код Грея по всем разбиениям α, таким, что $\lambda \preccurlyeq \alpha \preccurlyeq \mu$?

► **64.** [*32*] (*Бинарные разбиения.*) Разработайте алгоритм без применения циклов, который посещает все разбиения n на степени 2, где каждый шаг заменяет $2^k + 2^k$ на 2^{k+1} или наоборот.

65. [*23*] Хорошо известно, что каждая коммутативная группа из m элементов может быть представлена в виде дискретного тора $T(m_1, \ldots, m_n)$ с операцией сложения 7.2.1.3–(66), где $m = m_1 \ldots m_n$, а m_j кратно m_{j+1} при $1 \leqslant j < n$. Например, для $m = 360 = 2^3 \cdot 3^2 \cdot 5^1$ имеется шесть групп, соответствующих разложениям $(m_1, m_2, m_3) = (30, 6, 2)$, $(60, 6, 1)$, $(90, 2, 2)$, $(120, 3, 1)$, $(180, 2, 1)$ и $(360, 1, 1)$.

Поясните, как систематически сгенерировать все такие разложения при помощи алгоритма, который на каждом шаге изменяет ровно два множителя m_j.

► **66.** [*M25*] (*P-разбиения.*) Предположим, что вместо требования $a_1 \geqslant a_2 \geqslant \cdots$ мы рассматриваем все неотрицательные композиции n, удовлетворяющие некоторому заданному *частичному* порядку. Например, П.А. Мак-Мэган (P.A. MacMahon) заметил, что все решения "холмистых" (up-down) неравенств $a_4 \leqslant a_2 \geqslant a_3 \leqslant a_1$ можно разделить на пять неперекрывающихся типов:

$$a_1 \geqslant a_2 \geqslant a_3 \geqslant a_4; \quad a_1 \geqslant a_2 \geqslant a_4 > a_3;$$
$$a_2 > a_1 \geqslant a_3 \geqslant a_4; \quad a_2 > a_1 \geqslant a_4 > a_3; \quad a_2 \geqslant a_4 > a_1 \geqslant a_3.$$

Все эти типы легко перечислимы, поскольку, например, $a_2 > a_1 \geqslant a_4 > a_3$ эквивалентно $a_2 - 2 \geqslant a_1 - 1 \geqslant a_4 - 1 \geqslant a_3$; количество решений при $a_3 \geqslant 0$ и $a_1 + a_2 + a_3 + a_4 = n$ равно количеству разбиений $n - 1 - 2 - 0 - 1$ не более чем на четыре части.

Объясните, как решить общую задачу такого вида: дано отношение $\prec$ некоторого частичного порядка для m элементов. Рассмотрим все m-кортежи $a_1 \ldots a_m$ с тем свойством, что $a_j \geqslant a_k$, если $j \prec k$. Полагая, что индексы выбраны таким образом, что из $j \prec k$ вытекает $j \leqslant k$, покажите, что все соответствующие m-кортежи делятся на N классов, по одному для каждого из выходов алгоритма топологической сортировки 7.2.1.2V. Какой вид имеет производящая функция для всех неотрицательных $a_1 \ldots a_m$, сумма которых равна n? Каким образом можно сгенерировать их всех?

67. [*M25*] (П.А. Мак-Мэган (P.A. MacMahon), 1886.) *Идеальным разбиением* n является мультимножество, которое имеет ровно $n + 1$ подмультимножеств, и эти мультимножества представляют собой разбиения целых чисел $0, 1, \ldots, n$. Например, мультимножества $\{1, 1, 1, 1, 1\}$, $\{2, 2, 1\}$ и $\{3, 1, 1\}$ являются идеальными разбиениями 5.

Поясните, как построить идеальные разбиения n, имеющие наименьшее количество элементов.

68. [*M23*] Какое разбиение n на m частей имеет наибольшее произведение $a_1 \ldots a_m$ при (a) заданном m; (b) произвольном m?

69. [*M30*] Найдите все $n < 10^9$, такие, что уравнение $x_1 + x_2 + \cdots + x_n = x_1 x_2 \ldots x_n$ имеет единственное решение в натуральных числах $x_1 \geqslant x_2 \geqslant \cdots \geqslant x_n$. (Имеются, например, единственные решения для $n = 2, 3$ и 4; однако $5+2+1+1+1 = 5 \cdot 2 \cdot 1 \cdot 1 \cdot 1$, $3 + 3 + 1 + 1 + 1 = 3 \cdot 3 \cdot 1 \cdot 1 \cdot 1$ и $2 + 2 + 2 + 1 + 1 = 2 \cdot 2 \cdot 2 \cdot 1 \cdot 1$.)

70. [*M30*] ("*Болгарский пасьянс*".) Даны n карт, разделенные произвольным образом на одну или несколько стопок. Затем многократно выполняются следующие действия — из каждой стопки берется по одной карте, и они образуют новую стопку.

Покажите, что, если $n = 1 + 2 + \cdots + m$, этот процесс всегда достигает самовоспроизводящегося состояния со стопками размером $\{m, m-1, \ldots, 1\}$. например, если $n = 10$, и мы начинаем со стопок размером $\{3, 3, 2, 2\}$, то получим такую последовательность разбиений:

$$3322 \to 42211 \to 5311 \to 442 \to 3331 \to 4222 \to 43111 \to 532 \to 4321 \to 4321 \to \cdots .$$

Какие циклы состояний возможны для других значений n?

71. [*M46*] Продолжая предыдущее упражнение, чему равно максимальное количество шагов, которые могут быть выполнены до того, как Болгарский пасьянс с n картами достигнет циклического состояния?

72. [*M25*] Предположим, мы записали все разбиения n, например

$$6, 51, 42, 411, 33, 321, 3111, 222, 2211, 21111, 111111$$

для $n = 6$, и заменили все j-е появления числа k на j:

$$1, 11, 11, 112, 12, 111, 1123, 123, 1212, 11234, 123456.$$

a) Докажите, что эта операция порождает перестановку отдельных элементов.

b) Сколько всего раз встречается элемент k?