ОГЛАВЛЕНИЕ

ГЛАВА 3

СЛУЧАЙНЫЕ ЧИСЛА

Каждый, кто использует арифметические методы генерирования случайных чисел, безусловно, грешит.

— ДЖОН ФОН НЕЙМАН (JOHN VON NEUMANN) (1951)

О вероятности коль кто забудет, обманщиком вовек не будет.

— ДЖОН ГЕЙ (JOHN GAY) (1727)

Достаточно лишь нескольких лучей света, чтобы помочь людям в совершенствовании их "стохастических" способностей.

— ДЖОН ОУЭН (JOHN OWEN) (1662)

3.1. ВВЕДЕНИЕ

Числа, которые выбираются случайным образом, находят множество полезных применений.

a) *Моделирование.* При использовании компьютера для моделирования естественных явлений случайные числа нужны для того, чтобы сделать эти модели похожими на реальные явления. Моделирование применяется во многих областях, начиная от исследований в ядерной физике (где частицы испытывают случайные столкновения) и заканчивая исследованием операций (где люди прибывают, например, в аэропорт через случайные промежутки времени).

b) *Выборочный метод.* Часто невозможно исследовать все варианты, но случайная выборка обеспечивает понимание того, что можно назвать "типичным" поведением.

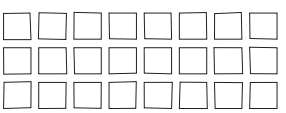
c) *Численный анализ.* Для решения сложных задач численного анализа была разработана остроумная техника, использующая случайные числа. Об этом написано несколько книг.

d) *Компьютерное программирование.* Случайные величины являются хорошим источником данных для тестирования эффективности компьютерных алгоритмов.

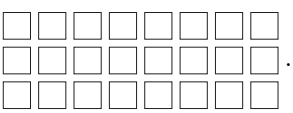
Более важно то, что они играют решающую роль при использовании *рандомизированных алгоритмов*, которые часто намного превосходят своих детерминированных двойников. В этой серии книг нас, в первую очередь, интересует именно такое использование случайных чисел. Этим объясняется то, что случайные числа рассматриваются уже здесь, в главе 3, прежде чем появится большинство других компьютерных алгоритмов.

e) *Принятие решений.* Говорят, что многие администраторы принимают решения, бросая монету, игральную кость либо каким нибудь другим подобным способом. Сплетничают, что некоторые профессора в колледжах ставят оценки, используя тот же метод. Иногда важно принять полностью "беспристрастное" решение. Случайность является также важной частью оптимальных стратегий в теории матричных игр.

f) *Эстетика.* Небольшая добавка случайности оживляет музыку и компьютерную графику. Например, рисунок



в определенном смысле выглядит привлекательнее, чем



.

[См. D. E. Knuth, *Bull. Amer. Math. Soc.* **1** (1979), 369.]

g) *Развлечения.* Многие считают, что они замечательно проводят время, бросая игральные кости, тасуя колоду карт, вращая колесо рулетки и т. п. Такие традиционные способы использования случайных чисел получили название *метод Монте–Карло.* Это общее название всех алгоритмов, использующих случайные числа.

Те же, кто интересуются этой темой, постоянно вовлекаются в философские дискуссии о значении слова "случайный". Возникает вопрос "А что является неслучайным числом?" Например, будет ли число 2 случайным? Охотнее говорят о *последовательности независимых случайных чисел* с заданным *распределением*, и это означает, если говорить не строго, что каждое число было получено случайно, не имея ничего общего с другими числами в последовательности, и что каждое число имеет заданную вероятность появления в любой заданной области значений.

Равномерным распределением на конечном множестве чисел (в дальнейшем — просто *равномерным распределением*) называется такое распределение, при котором любое из возможных чисел имеет одинаковую вероятность появления. Если не задано определенное распределение на конечном множестве чисел, то принято считать его равномерным.

Каждая из десяти цифр от 0 до 9 будет появляться примерно один раз из 10 в равномерной последовательности случайных цифр. Каждой паре двух последовательных цифр следует появиться один раз из ста и т. д. Однако если взять конкретную случайную последовательность длиной в миллион цифр, то она не всегда будет содержать 100 000 нулей, 100 000 единиц и т. д. Действительно, возможность появления такой последовательности незначительна; на самом деле, если рассматривать достаточно большую совокупность таких *последовательностей*, в среднем будет появляться 100 000 нулей, 100 000 единиц и т. д.

Любая конкретная последовательность, содержащая миллион цифр, так же вероятна, как и любая другая. Если мы выберем миллион цифр наудачу и если

окажется, что первые 999 999 из них — нули, то вероятность того, что последняя цифра в этой последовательности — также нуль, все еще остается точно равной одной десятой в истинно случайной ситуации. Это утверждение большинству кажется парадоксальным, однако оно не противоречит реальности.

Существует несколько приличных возможностей дать абстрактное определение случайности, и мы вернемся к этой интересной теме в разделе 3.5; пока что достаточно интуитивного понимания данной концепции.

В течение многих лет те, кому случайные числа были необходимы для научной работы, вынуждены были таскать шары из урны, предварительно хорошо перемешав их, либо бросать игральные кости, либо раскладывать карты. Таблица, содержащая более 40 000 взятых наудачу из отчетов о переписи случайных цифр, была опубликована в 1927 году Л. Х. К. Типпеттом (L. H. C. Tippett).

С тех пор были построены механические генераторы случайных чисел. Первая такая машина была использована в 1939 году М. Ж. Кендаллом (M. G. Kendall) и Б. Бабингтон-Смитом (B. Babington-Smith) для построения таблицы, содержащей 100 000 случайных цифр. Компьютер Ferranti Mark I, впервые запущенный в 1951 году, имел встроенную программу, использующую резисторный генератор шума, которая поставляла 20 случайных битов на сумматор. Этот метод был предложен А. М. Тьюрингом (A. M. Turing). В 1955 году RAND Corporation опубликовала широко используемые таблицы, в которых содержался миллион случайных цифр, полученных с помощью других специальных устройств. Известный генератор случайных чисел ERNIE применялся на протяжении многих лет для определения выигрышных номеров британской лотереи. [См. статьи Kendall and Babington-Smith *J. Royal Stat. Soc.* **A101** (1938), 147–166; **B6** (1939), 51–61, а также дискуссию S. H. Lavington's с Mark I в *CACM* **21** (1978), 4–12; обозрение в *Math. Comp.* **10** (1956), 39–43; дискуссию об ERNIE W. E. Thomson, *J. Royal Stat. Soc.* **A122** (1959), 301–333.]

Короче говоря, после изобретения компьютеров начались исследования эффективного способа получения случайных чисел, встроенных программно в компьютеры. Можно было применять таблицы, но пользы от этого метода было мало из-за ограниченной памяти компьютера и требуемого времени ввода, поэтому таблицы могли быть лишь слишком короткими; кроме того, было не особенно приятно составлять таблицы и пользоваться ими. Генератор ERNIE мог быть встроен в компьютер, как это было в Ferranti Mark I, но это оказалось неудобно, поскольку невозможно точно воспроизвести вычисления даже сразу по окончании работы программы; более того, такие генераторы часто давали сбои, что было крайне трудно обнаружить. Технологический прогресс позволил вернуться к использованию таблиц в 1990-е годы, так как миллиарды протестированных случайных байтов можно было разместить на компакт-дисках. Дж. Марсалья (George Marsaglia) помог оживить табличный метод в 1995 году, подготовив демонстрационный диск с 650 Мбайт случайных чисел, при генерировании которых запись шума диодной цепи сочеталась с определенным образом скомпонованной музыкой в стиле "рэп". (Он назвал это "белым и черным шумом".)

Несовершенство первых механических методов вначале пробудило интерес к получению случайных чисел с помощью обычных арифметических операций, заложенных в компьютер. Джон фон Нейман (John von Neumann) первым предложил

такой подход около 1946 года; его идея заключалась в том, чтобы возвести в квадрат предыдущее случайное число и выделить средние цифры. Например, мы хотим получить 10-значное число и предыдущее число равнялось 5772156649. Возводим его в квадрат и получаем

$$33317792380594909201;$$

значит, следующим числом будет 7923805949.

Совершенно очевидны претензии, предъявляемые к этому методу: как может быть случайной последовательность, генерируемая таким образом, если каждое число полностью определяется предыдущим? (См. эпиграф фон Неймана к этой главе.) Ответ состоит в том, что эта последовательность *не* случайна, но *кажется* такой. В типичных приложениях фактически существующая связь между двумя числами, следующими одно за другим, на самом деле не имеет значения; поэтому нельзя утверждать, что неслучайный характер последовательности нежелателен. Интуитивно ясно, что метод средин квадратов должен быть достаточно хорошим перемешиванием и заменой цифр предыдущего числа.

В "заумной" технической литературе последовательности, генерируемые детерминистическим путем, таким как этот, называются *псевдослучайными* или *квазислучайными*, однако в данной книге мы в основном просто будем называть их случайными последовательностями, понимая, что они только *кажутся* случайными. "Кажущаяся случайность" — это, возможно, все, что так или иначе может быть сказано о любой случайной последовательности. Случайные числа, генерируемые детерминистическими методами на компьютере, почти всегда работали достаточно хорошо при условии, что метод был выбран удачно. Конечно, детерминистическая последовательность не всегда применима; ею, безусловно, не следует заменять ERNIE в лотерее.

Метод средин квадратов фон Неймана, как было показано, фактически является сравнительно бедным источником случайных чисел. Опасность состоит в том, что последовательность стремится войти в привычную колею, т. е. короткий цикл повторяющихся элементов. Например, каждое появление нуля как числа последовательности приведет к тому, что все последующие числа также будут нулями.

Некоторые ученые экспериментировали с методом средин квадратов в начале 1950-х годов. Работая с четырехзначными числами вместо десятизначных, Дж. Э. Форсайт (G. E. Forsythe) испытал 16 различных начальных значений и обнаружил, что 12 из них приводят к циклическим последовательностям, заканчивающимся циклом 6100, 2100, 4100, 8100, 6100, ..., в то время как две из них приводят к последовательностям, вырождающимся в 0. Более интенсивные исследования, главным образом в двоичной системе счисления, провел Н. К. Метрополис (N. C. Metropolis). Он показал, что если использовать 20-разрядное число, то последовательность случайных чисел, полученная методом средин квадратов, вырождается в 13 различных циклов, причем длина самого большого периода равна 142.

Достаточно легко запустить метод средин квадратов с новым исходным значением, если обнаружить число "нуль", однако избавиться от длинных циклов довольно трудно. В упр. 6 и 7 обсуждается несколько интересных вариантов определения циклов периодических последовательностей, использующих достаточно малый объем памяти.

Теоретические недостатки метода средин квадратов приведены в упр. 9 и 10. С другой стороны, используя 38-разрядные числа, Метрополис получил невырожденную последовательность, содержащую около 750 000 чисел (прежде чем произошло вырождение), и полученные $750\,000 \times 38$ бит удовлетворительно прошли статистический тест на случайность. [*Symp. on Monte Carlo Methods* (Wiley, 1956), 29–36.] Эти опыты показали, что метод средин квадратов *может* давать удовлетворительные результаты, но ему опасно доверять, пока не выполнены тщательные вычисления.

Когда автор работал над первым изданием этой книги, многие генераторы случайных чисел (в литературе на русском языке параллельно употребляется термин "датчик случайных чисел". — *Примеч. ред.*), которые тогда использовались, были недостаточно хороши. Программисты традиционно не интересовались информацией о таких подпрограммах; старые методы, сравнительно неудовлетворительные, слепо переходили от одного программиста к другому, поскольку пользователи не понимали ограничений, при которых можно применять эти методы. Мы увидим здесь, что наиболее важные сведения о генераторах случайных чисел нетрудно изучить, несмотря на то что необходимо быть осторожным, чтобы избежать обычных ловушек.

Так нелегко придумать понятный всем и каждому датчик случайных чисел! В этом автор убедился в 1959 году, когда попытался создать фантастически хороший генератор случайных чисел, используя следующий необычный подход.

Алгоритм К (*Супергенератор случайных чисел*). Пусть задано 10-значное десятичное число X и этот алгоритм использует замену X другим числом так, чтобы получить случайную последовательность. Несмотря на то что от алгоритма можно ожидать на выходе всецело случайную последовательность, соображения, приведенные ниже, показывают, что это, к сожалению, не всегда так. (Читатель не обязан изучать этот алгоритм во всех деталях, но рекомендуется обратить внимание на его сложность; отметим, в частности, шаги К1 и К2.)

К1. [Выбрать число итераций.] Присвоить $Y \leftarrow \lfloor X/10^9 \rfloor$ наибольшую значащую цифру X. (Мы выполним шаги К2–К13 точно $Y + 1$ раз; т. е. применим рандомизированные преобразования *случайное* число раз.)

К2. [Выбрать случайный шаг.] Присвоить $Z \leftarrow \lfloor X/10^8 \rfloor \bmod 10$ следующую наибольшую значащую цифру X. Переходим к шагу К$(3 + Z)$, т. е. к *случайно* выбранному шагу в программе.

К3. [Обеспечить $\geq 5 \times 10^9$.] Если $X < 5000000000$, присвоить $X \leftarrow X + 5000000000$.

К4. [Средина квадрата.] Заменить X числом $\lfloor X^2/10^5 \rfloor \bmod 10^{10}$, т. е. серединой квадрата X.

К5. [Умножить.] Заменить X числом $(1001001001\,X) \bmod 10^{10}$.

К6. [Псевдодополнение.] Если $X < 100000000$, то присвоить $X \leftarrow X + 9814055677$; иначе присвоить $X \leftarrow 10^{10} - X$.

К7. [Переставить половины.] Поменять местами пять младших по порядку знаков X со старшими по порядку пятью знаками, т. е. присвоить $X \leftarrow 10^5(X \bmod 10^5) + \lfloor X/10^5 \rfloor$; это то же самое, что взять десять средних цифр числа $(10^{10} + 1)X$.

К8. [Умножить.] Выполнить шаг К5.

Таблица 1

КОЛОССАЛЬНОЕ СОВПАДЕНИЕ: АЛГОРИТМ К ПРЕОБРАЗОВАЛ ЧИСЛО 6065038420 САМО В СЕБЯ

Шаг	X (после)	
К1	6065038420	
К3	6065038420	
К4	6910360760	
К5	8031120760	
К6	1968879240	
К7	7924019688	
К8	9631707688	
К9	8520606577	
К10	8520506578	
К11	8520506578	
К12	0323372207	$Y = 6$
К6	9676627793	
К7	2779396766	
К8	4942162766	
К9	3831051655	
К10	3830951656	
К11	3830951656	
К12	1905867781	$Y = 5$
К12	3319967479	$Y = 4$
К6	6680032521	
К7	3252166800	
К8	2218966800	
К9	1107855700	
К10	1107755701	
К11	1107755701	
К12	1226919902	$Y = 3$
К5	0048821902	
К6	9862877579	
К7	7757998628	
К8	2384626628	
К9	1273515517	
К10	1273415518	
К11	1273415518	
К12	5870802097	$Y = 2$
К11	5870802097	
К12	3172562687	$Y = 1$
К4	1540029446	
К5	7015475446	
К6	2984524554	
К7	2455429845	
К8	2730274845	
К9	1620163734	
К10	1620063735	
К11	1620063735	
К12	6065038420	$Y = 0$

К9. [Уменьшить цифры.] Уменьшить каждую не равную нулю цифру десятичного представления числа X на единицу.

К10. [Модифицировать на 99999.] Если $X < 10^5$, присвоить $X \leftarrow X^2 + 99999$; иначе присвоить $X \leftarrow X - 99999$.

К11. [Нормировать.] (На этом шаге X не может быть равным нулю.) Если $X < 10^9$, присвоить $X \leftarrow 10X$ и повторить этот шаг.

К12. [Модификация метода средин квадратов.] Заменить X на $\lfloor X(X-1)/10^5 \rfloor \bmod 10^{10}$, т. е. средними 10 цифрами числа $X(X-1)$.

К13. [Повторить?] Если $Y > 0$, уменьшить Y на 1 и возвратиться к шагу К2. Если $Y = 0$, алгоритм завершен. Значение числа X, полученное на предыдущем шаге, и будет желаемым "случайным" значением. ▮

(Программа, реализующая этот алгоритм, обещала быть настолько сложной, что тот, кто прочел бы ее распечатку, без толковых комментариев не смог бы в ней разобраться.)

После рассмотрения всех преобразований алгоритма К не кажется ли правдоподобным, что можно было бы обеспечить бесконечное снабжение невероятно случайными числами? Нет! На самом деле, когда этот алгоритм впервые был реализован на компьютере, он почти немедленно сошелся к 10-значному числу 6065038420,

которое по невероятному совпадению преобразовалось само в себя по алгоритму (табл. 1). С другим стартовым числом последовательность начала повторяться после 7401 значения с периодом длиной 3178.

Мораль этой истории в том, что *случайные числа не следует генерировать методом, выбранным наудачу*. Не мешало бы использовать немного теории.

В следующих разделах будут рассмотрены генераторы случайных чисел более высокого уровня, чем метод средин квадратов и алгоритм K. Соответствующие последовательности гарантированно обладают желаемыми случайными свойствами и не вырождаются. Мы исследуем некоторые причины такого, похожего на случайное, поведения, а также покажем, как можно обращаться со случайными числами. Например, одно из наших исследований будет посвящено программе, которая тасует смоделированную на компьютере колоду карт.

В разделе 3.6 приводятся итоги к этой главе и некоторые библиографические источники.

УПРАЖНЕНИЯ

▸ **1.** [*20*] Предположим, вы хотите получить случайную десятичную цифру. Какой из следующих методов вы выберете?

a) Откроете телефонный справочник, ткнув пальцем куда-нибудь, выберете первый попавшийся номер телефона и возьмете младшую цифру (*цифру младшего разряда*) этого номера.
b) Поступите, как в (a), но выберете младшую цифру номера *страницы*.
c) Бросите игральную кость в форме икосаэдра, имеющую двадцать граней, которые помечены цифрами $0, 0, 1, 1, \ldots, 9, 9$. Когда кость остановится, выберете верхнюю цифру. (Для бросания игральной кости рекомендуется стол с хорошо натянутым сукном.)
d) На одну минуту выставите счетчик Гейгера у источника радиоактивного излучения (предварительно обезопасив себя) и воспользуетесь младшей цифрой показаний счетчика. Предполагается, что на счетчике Гейгера представлены числа в десятичной системе счисления и вначале на нем был установлен нуль.
e) Бросите быстрый взгляд на свои часы и, если секундная стрелка находится между $6n$ и $6(n+1)$ секундами, выберете цифру n.
f) Попросите приятеля задумать любую цифру и воспользуетесь ею.
g) Попросите врага задумать любую цифру и воспользуетесь ею.
h) Предположите, что 10 лошадей участвуют в забеге и вам о них абсолютно ничего не известно. Присвоите каждой лошади в произвольном порядке номер от 0 до 9, а после забега выберете в качестве случайной цифры номер победителя.

2. [*M22*] Какова вероятность того, что в случайной последовательности из миллиона десятичных цифр каждая возможная цифра встречается ровно 100 000 раз?

3. [*10*] Какое число следует за 1010101010 в методе средин квадратов?

4. [*20*] (a) Почему на шаге K11 алгоритма K значение X не может быть равно нулю? Какая ошибка возникла бы в алгоритме, если бы X мог принимать значение "нуль"? (b) Используя табл. 1, установите, что происходит, когда алгоритм K применяется повторно со стартовым значением $X = 3830951656$.

5. [*15*] Объясните, почему в любом случае, даже если совпадение, приведенное в табл. 1, не произошло, алгоритм K не сможет выдать бесконечную последовательность случайных чисел в том смысле, что любая последовательность, генерируемая алгоритмом K, станет в конце концов периодичной.

▸ **6.** [*M21*] Предположим, что необходимо получить последовательность целых случайных чисел X_0, X_1, X_2, ... на интервале $0 \le X_n < m$. Пусть $f(x)$ — любая функция, такая, что неравенство $0 \le x < m$ влечет $0 \le f(x) < m$. Рассмотрим последовательность $X_{n+1} = f(X_n)$. (Примеры таких последовательностей — метод средин квадратов и алгоритм К.)

a) Покажите, что такая последовательность периодична в том смысле, что существуют числа λ и μ, для которых значения

$$X_0,\ X_1,\ \ldots,\ X_\mu,\ \ldots, X_{\mu+\lambda-1}$$

различны, однако $X_{n+\lambda} = X_n$, когда $n \ge \mu$. Определите возможные максимальное и минимальное значения μ и λ.

b) (Р. В. Флойд (R. W. Floyd).) Покажите, что существует такое $n > 0$, что $X_n = X_{2n}$, и наименьшее такое значение n лежит в интервале $\mu \le n \le \mu + \lambda$. Более того, значение X_n является единственным в том смысле, что если $X_n = X_{2n}$ и $X_r = X_{2r}$, то $X_r = X_n$.

c) Используя идеи (b), составьте алгоритм вычисления μ и λ для любой заданной функции f и любого заданного X_0, используя только $O(\mu+\lambda)$ шагов и только ограниченный объем памяти.

▸ **7.** [*M21*] (Р. П. Брент (R. P. Brent), 1977.) Пусть $\ell(n)$ — наибольшее целое число, такое, что $2^{\ell(n)} \le n$, $\ell(n) = 2^k$, где k — целое число. Так, например, $\ell(15) = 8$ и $\ell(\ell(n)) = \ell(n)$.

a) Покажите, что в терминах обозначений упр. 6 существует такое $n > 0$, что $X_n = X_{\ell(n)-1}$. Найдите формулу для наименьшего такого n в терминах чисел μ и λ, определяющих период.

b) Примените этот результат для составления алгоритма, который может быть использован совместно с любым генератором случайных чисел типа $X_{n+1} = f(X_n)$, чтобы предотвратить циклическую неопределенность. Вашему алгоритму следует вычислять период длиной λ и использовать только небольшой объем памяти — вы просто не должны заполнять всю память вычисленными значениями последовательности!

8. [*23*] Выполните полную проверку метода средин квадратов для случая, когда десятичные числа состоят из двух цифр.

a) Можете начать процесс с любого из 100 допустимых чисел 00, 01, ..., 99. Сколько из этих значений в конечном счете приведут к повторению цикла (зацикливанию) 00, 00, ...? [*Пример.* Начиная с числа 43, получим последовательность 43, 84, 05, 02, 00, 00, 00, ...]

b) Сколько существует финальных циклов? Каков размер самого длинного цикла?

c) Какое начальное значение (или значения) даст наибольшее число различных элементов, прежде чем последовательность повторится?

9. [*M14*] Докажите, что метод средин квадратов, использующий $2n$-значные числа в b-ичной системе счисления, имеет следующие недостатки: если последовательность включает любое число, в котором n старших значащих цифр — нули, то последующие числа становятся все меньше и меньше, пока не превратятся в нули.

10. [*M16*] Пусть выполняются предположения предыдущего упражнения. Что можно сказать о последовательности чисел, следующих за X, если *младшие* значащие n цифр числа X равны нулю? Что если $n+1$ младших значащих цифр равны нулю?

▸ **11.** [*M26*] Рассмотрим последовательности генераторов случайных чисел, имеющих вид, описанный в упр. 6. Если выбрать $f(x)$ и X_0 наудачу (другими словами, если предположить, что каждая из m^m возможных функций $f(x)$ равновероятна и каждое из m возможных значений X_0 равновероятно), то какова вероятность того, что последовательность в конечном счете выродится в цикл длиной $\lambda = 1$? [*Замечание.* Предположения этой задачи дают повод задуматься о "случайности" генераторов случайных чисел такого типа. Можно

ожидать, что метод, подобный алгоритму K, отчасти ведет себя так же, как рассмотренный здесь генератор; ответ на эту задачу дает колоссальное число совпадений в табл. 1.]

▸ **12.** [*M31*] Какова средняя длина финального цикла, если выполняются предположения предыдущего упражнения? Какова средняя длина последовательности до вхождения в цикл? (В обозначениях упр. 6 необходимо определить средние значения λ и $\mu + \lambda$.)

13. [*M42*] Если $f(x)$ выбрана наудачу, как в упр. 11, какова средняя длина самого *длинного* цикла, полученного путем варьирования начального значения X_0? [*Замечание.* Мы уже рассмотрели аналогичную проблему для случая, когда $f(x)$ — это случайные перестановки; см. упр. 1.3.3–23.]

14. [*M38*] Если $f(x)$ выбрано наудачу, как в упр. 11, каково среднее число различных финальных циклов, полученных в результате варьирования начальных значений? [См. упр. 8, (b).]

15. [*M15*] Если $f(x)$ выбрано наудачу, как и в упр. 11, чему равна вероятность, что ни один из финальных циклов не имеет длину, равную 1, невзирая на выбор X_0?

16. [*15*] Последовательность, генерируемая, как в упр. 6, должна повторяться после того, как было сгенерировано не более m значений. Предположим, что мы обобщим метод таким образом, что X_{n+1} будет зависеть от X_{n-1} так же, как от X_n; формально пусть $f(x, y)$ — такая функция, для которой $0 \le x, y < m$ влечет неравенства $0 \le f(x, y) < m$. Последовательность строится так: сначала произвольно выбирают X_0 и X_1, а затем полагают, что

$$X_{n+1} = f(X_n, X_{n-1}), \qquad \text{где } n > 0.$$

Чему предположительно равен максимальный период в этом случае?

17. [*10*] Обобщите ситуацию из предыдущего упражнения так, чтобы X_{n+1} зависело от предыдущих k значений последовательности.

18. [*M20*] Придумайте метод, аналогичный методу из упр. 7, для определения цикла генератора случайных чисел, описанного в упр. 17, в общем виде.

19. [*M48*] Выполните упр. 11, используя упр. 15, в более общем случае, когда X_{n+1} зависят от k предыдущих значений последовательности; каждая из m^{m^k} функций $f(x_1, \ldots, x_k)$ считается равновероятной. [*Замечание.* Число функций, которые дают *максимальный* период, анализируется в упр. 2.3.4.2–23.]

20. [*30*] Найдите все неотрицательные числа $X < 10^{10}$, которые при использовании алгоритма K в конечном счете приводят к самовоспроизводящимся числам из табл. 1.

21. [*42*] Докажите или опровергните следующее утверждение: отображение $X \mapsto f(X)$, определенное алгоритмом K, имеет ровно пять циклов длиной 3178, 1606, 1024, 943 и 1.

22. [*21*] (Г. Роллетшек (H. Rolletschek).) Хороша ли идея генерирования случайных чисел с помощью последовательности $f(0)$, $f(1)$, $f(2)$, ..., где f — случайная функция, вместо того, чтобы использовать x_0, $f(x_0)$, $f(f(x_0))$ и т. д.?

▸ **23.** [*M26*] (Д. Фоата (D. Foata) и А. Фучс (A. Fuchs), 1970.) Покажите, что каждая из m^m функций $f(x)$, рассмотренных в упр. 6, может быть представлена как последовательность $(x_0, x_1, \ldots, x_{m-1})$, имеющая такие свойства.

i) $(x_0, x_1, \ldots, x_{m-1})$ — это перестановки последовательности $\big(f(0), f(1), \ldots, f(m-1)\big)$.
ii) $\big(f(0), \ldots, f(m-1)\big)$ может быть единственным образом восстановлена из последовательности $(x_0, x_1, \ldots, x_{m-1})$.
iii) Элементы, которые появляются в циклах из f, имеют вид $\{x_0, x_1, \ldots, x_{k-1}\}$, где k — самый большой индекс, такой, что эти k элементов различны.
iv) $x_j \notin \{x_0, x_1, \ldots, x_{j-1}\}$ влечет $x_{j-1} = f(x_j)$, если x_j не является наименьшим элементом в цикле из f.

v) $(f(0), f(1), \ldots, f(m-1))$ — это перестановка последовательности $(0, 1, \ldots, m-1)$ тогда и только тогда, когда $(x_0, x_1, \ldots, x_{m-1})$ представляет собой *обратную* перестановку к той перестановке, которая в разделе 1.3.3 названа необычным соответствием.

vi) $x_0 = x_1$ тогда и только тогда, когда $(x_1, \ldots, x_{m-1})$ представляет собой ориентированное дерево, построенное в упр. 2.3.4.4–18, с $f(x)$, порождающим x.