3.2. ГЕНЕРИРОВАНИЕ РАВНОМЕРНО РАСПРЕДЕЛЕННЫХ СЛУЧАЙНЫХ ЧИСЕЛ

В ЭТОМ РАЗДЕЛЕ будут рассмотрены методы генерирования последовательности случайных дробей, т. е. случайных *действительных чисел U_n, равномерно распределенных между нулем и единицей (на интервале* $[0, 1)$*)*. Так как компьютер может представлять действительные числа только с определенной точностью, мы будем генерировать целое число X_n между нулем и некоторым числом m: дробь

$$U_n = X_n/m$$

будет, следовательно, лежать между нулем и единицей. Обычно m выбирают равным размеру слова в компьютере. (В этой книге размером слова (*word size*) автор называет число b^e, где b — основание системы счисления, используемой в компьютере, а e — число разрядов машины. — *Прим. ред.*) Поэтому X_n можно по традиции рассматривать как целое число, занимающее все компьютерное слово, с точкой, которая отделяет целую часть числа от дробной, стоящей в правом конце слова, а U_n — если хотите, как содержание того же слова с разделяющей точкой, стоящей в левом конце слова.

3.2.1. Линейный конгруэнтный метод

В настоящее время наиболее популярными генераторами случайных чисел являются генераторы, в которых используется следующая схема, предложенная Д. Г. Лехмером (D. H. Lehmer) в 1949 году [см. Proc. 2nd Symp. on Large-Scale Digital Calculating Machinary (Cambridge, Mass.: Harvard University Press, 1951, 141–146)]. Выберем четыре "волшебных числа":

$$\begin{array}{rll} m, & \text{модуль;} & 0 < m; \\ a, & \text{множитель;} & 0 \le a < m; \\ c, & \text{приращение;} & 0 \le c < m; \\ X_0, & \text{начальное значение;} & 0 \le X_0 < m. \end{array} \tag{1}$$

Затем получим желаемую последовательность случайных чисел $\langle X_n \rangle$, полагая

$$X_{n+1} = (aX_n + c) \bmod m, \qquad n \ge 0. \tag{2}$$

Эта последовательность называется *линейной конгруэнтной последовательностью*. Получение остатков по модулю m отчасти напоминает предопределенность, когда шарик попадает в ячейку крутящегося колеса рулетки. Например, для $m = 10$ и $X_0 = a = c = 7$ получим последовательность

$$7,\ 6,\ 9,\ 0,\ 7,\ 6,\ 9,\ 0,\ \ldots\ . \tag{3}$$

Как показывает этот пример, такая последовательность не может быть "случайной" при некоторых наборах чисел m, a, c и X_0. Принципы выбора подходящих волшебных чисел будут подробно исследованы в следующих разделах этой главы.

В примере (3) иллюстрируется тот факт, что конгруэнтная последовательность всегда образует петли, т. е. обязательно существует цикл, повторяющийся бесконечное число раз. Это свойство является общим для всех последовательностей вида $X_{n+1} = f(X_n)$, где f преобразует конечное множество само в себя (см. упр. 3.1–6).

Повторяющиеся циклы называются *периодами*; длина периода последовательности (3) равна 4. Безусловно, последовательности, которые мы будем использовать, имеют относительно длинный период.

Заслуживает внимания случай, когда $c = 0$, так как генерируемые числа будут иметь меньший период, чем при $c \neq 0$. Мы убедимся в дальнейшем, что ограничение $c = 0$ уменьшает длину периода последовательности, хотя при этом все еще возможно сделать период достаточно длинным. В оригинальном методе, предложенном Д. Г. Лехмером, c выбиралось равным нулю, хотя он и допускал случай, когда $c \neq 0$, как один из возможных. Тот факт, что условие $c \neq 0$ может приводить к появлению более длинных периодов, был установлен В. Е. Томсоном (W. E. Thomson) [Comp. J. 1 p. 83, 86] и независимо от него А. Ротенбергом (A. Rotenberg) [JACM 7 (1960), 75–77]. Многие авторы называют линейную конгруэнтную последовательность при $c = 0$ *мультипликативным конгруэнтным методом*, а при $c \neq 0$ — *смешанным конгруэнтным методом*. Буквы m, a, c и X_0 будут использованы в этой главе в том смысле, в каком они вводились раньше. То же самое относится и к константе

$$b = a - 1, \tag{4}$$

которая вводится для упрощения многих наших формул.

Можно сразу отбросить случай, когда $a = 1$, при котором последовательность X_n представима в виде $X_n = (X_0 + nc) \bmod m$ и ведет себя явно не как случайная последовательность. Случай, когда $a = 0$, даже хуже предыдущего. Следовательно, для практических целей предполагаем, что

$$a \geq 2, \qquad b \geq 1. \tag{5}$$

Сейчас можно обобщить формулу (2)

$$X_{n+k} = \big(a^k X_n + (a^k - 1)c/b\big) \bmod m, \qquad k \geq 0, \quad n \geq 0, \tag{6}$$

где $(n + k)$-й член выражается непосредственно через n-й. (Случай, когда $n = 0$, в этом уравнении также достоин внимания.) Из (4) следует, что подпоследовательность, содержащая каждый k-й член последовательности $\langle X_n \rangle$, является также линейной конгруэнтной последовательностью, множитель которой равен $a^k \bmod m$ и приращение равно $\big((a^k - 1)c/b\big) \bmod m$. Важным следствием из (6) является то, что общая последовательность, определенная с помощью a, c и X_0, может быть очень просто выражена в терминах специального случая, когда $c = 1$ и $X_0 = 0$. Пусть

$$Y_0 = 0, \qquad Y_{n+1} = (aY_n + 1) \bmod m. \tag{7}$$

В соответствии с (6) получим $Y_k \equiv (a^k - 1)/b$ (по модулю m). Значит, последовательность, определенная в (2), будет имеет вид

$$X_n = (AY_n + X_0) \bmod m, \qquad \text{где } A = (X_0 b + c) \bmod m. \tag{8}$$

УПРАЖНЕНИЯ

1. [*10*] В примере (3) показана ситуация, когда $X_4 = X_0$, так что последовательность начинается сначала. Приведите пример линейной конгруэнтной последовательности при $m = 10$, для которой число X_0 никогда снова не появится.

▸ **2.** [*M20*] Покажите, что если a и m взаимно простые, то X_0 всегда появится в периоде.

3. [*M10*] Объясните, почему последовательность имеет определенные недостатки и, вероятно, не очень случайна, если a и m — не взаимно простые числа. Поэтому следует выбирать a и m так, чтобы они были взаимно простыми.

4. [*11*] Докажите формулу (6).

5. [*M20*] Соотношение (6) справедливо при $k \geq 0$. Если это возможно, получите формулы для X_{n+k} в терминах X_n для *отрицательных* значений k.

3.2.1.1. Выбор модуля. Первая задача, которую мы рассмотрим, — нахождение хороших значений параметров, определяющих линейную конгруэнтную последовательность. Сначала выясним, как правильно выбрать число m. Необходимо, чтобы m было довольно большим, так как период не может иметь больше m элементов. (Даже если мы намерены генерировать только случайные нули и единицы, *не* следует брать $m = 2$, ибо тогда последовательность в лучшем случае будет иметь вид $\ldots, 0, 1, 0, 1, 0, 1, \ldots$! Методы получения случайных нулей и единиц из линейной конгруэнтной последовательности обсуждаются в разделе 3.4.)

Другой фактор, который оказывает влияние на выбор m, — скорость генерирования: нужно подобрать значение m так, чтобы $(aX_n + c) \bmod m$ вычислялось быстро.

В качестве примера рассмотрим компьютер MIX. Можно вычислить $y \bmod m$, помещая y в регистры A и X и выполняя деление на m. Если y и m положительны, то $y \bmod m$ появится в регистре X. Но деление — сравнительно медленно протекающая операция, и этот недостаток можно компенсировать, если выбрать значение m таким, что особенно удобно, как *длина слова* нашего компьютера.

Пусть w будет длиной компьютерного слова, а именно — 2^e на e-разрядном двоичном компьютере или 10^e на e-цифровой десятичной вычислительной машине. (В настоящей книге мы часто будем употреблять букву e для обозначения произвольной целой степени. Несмотря на то что эта буква часто используется для обозначения основания натурального логарифма, мы надеемся, что читателю из контекста будет понятно, что она обозначает. Физики сталкиваются с подобными проблемами, когда используют e для обозначения заряда электрона.) Результат операции суммирования обычно дается по модулю w (но не на машинах, использующих процедуру единичного дополнения); умножение по модулю w также очень простое, поскольку затрагиваются только младшие разряды произведения. Таким образом, следующая программа эффективно вычисляет величину $(aX + c) \bmod w$.

```
LDA   A     rA ← a.
MUL   X     rAX ← (rA) · X.
SLAX  5     rA ← rAX mod w.                    (1)
ADD   C     rA ← (rA + c) mod w.   ∎
```

Результат появляется в регистре A. В конце программы возможно переполнение; если это нежелательно, то следует, допустим, команда "JOV *+1" — "выключить".

"Умная" техника, обычно менее известная, может использовать представление вычисления по модулю $w + 1$. По причинам, поясняемым ниже, как правило, требуется, чтобы $c = 0$, когда $m = w + 1$; тогда мы просто должны вычислить

$(aX) \bmod (w+1)$. Делает это следующая программа.

```
01  LDAN X         rA ← −X.
02  MUL  A         rAX ← (rA) · a.
03  STX  TEMP
04  SUB  TEMP      rA ← rA − rX.                    (2)
05  JANN *+3       Выход, если rA ≥ 0.
06  INCA 2         rA ← rA + 2.
07  ADD  =w−1=     rA ← rA + w − 1.   ▮
```

В регистре A сейчас содержится значение $(aX) \bmod (w+1)$. Конечно, оно может лежать где-нибудь между 0 и w включительно, так что читатель может законно удивиться, как можно представить так много значений в регистре A! (Обычно регистр не может хранить число, большее, чем $w-1$.) Ответом является то, что переполнение в программе (2) происходит тогда и только тогда, когда результат равен w (если предположить, что переполнение убрано в исходном положении). Можно отобразить w в виде нуля, так как программу (2) обычно нельзя использовать, когда $X = 0$; но более удобно просто отбросить значение w, если оно появляется в конгруэнтной последовательности по модулю $w+1$. Затем также можно избежать переполнения, просто заменив строки 05 и 06 в (2) строками "`JANN *+4; INCA 2; JAP *-5`".

Для доказательства того, что программа (2) действительно вычисляет $(aX) \bmod (w+1)$, заметим, что в строке 04 младшие разряды произведения вычитаются из старших разрядов. Переполнение не может произойти на этом шаге, и, если $aX = qw + r$ при $0 \le r < w$, получим значение $r - q$ в регистре A после строки 04. Сейчас

$$aX = q(w+1) + (r-q)$$

и мы имеем $-w < r - q < w$, так как $q < w$; следовательно, $(aX) \bmod (w+1)$ равно одному из двух значений ($r-q$ или $r-q+(w+1)$) в зависимости от того, $r - q \ge 0$ или $r - q < 0$.

Подобная техника может быть использована для получения произведения двух чисел по модулю $(w-1)$; см. упр. 8.

Для освоения следующих разделов требуется знать простые множители m, чтобы правильно выбрать a. В табл. 1 впервые дается полный список разложений на простые множители $w \pm 1$ почти для каждой известной длины компьютерного слова; при желании методы из раздела 4.5.4 можно использовать для расширения таблицы.

Читатель может поинтересоваться, почему здесь обсуждается использование $m = w \pm 1$, когда выбор $m = w$ так явно удобен. Причина в том, что, *когда $m = w$, цифры правой части X_n гораздо менее случайны, чем цифры левой части.* Если d является делителем m и если

$$Y_n = X_n \bmod d, \tag{3}$$

можно легко показать, что

$$Y_{n+1} = (aY_n + c) \bmod d. \tag{4}$$

(Пусть $X_{n+1} = aX_n + c - qm$, где q — некоторое целое число. Если обе части равенства взять по модулю d, можно потерять qm, когда d — множитель m.)

Для иллюстрации важности выражения (4) предположим, например, что имеется двоичный компьютер. Если $m = w = 2^e$, младшие четыре разряда X_n являются

Таблица 1

РАЗЛОЖЕНИЕ НА ПРОСТЫЕ МНОЖИТЕЛИ $w \pm 1$

$2^e - 1$	e	$2^e + 1$
$7 \cdot 31 \cdot 151$	15	$3^2 \cdot 11 \cdot 331$
$3 \cdot 5 \cdot 17 \cdot 257$	16	65537
131071	17	$3 \cdot 43691$
$3^3 \cdot 7 \cdot 19 \cdot 73$	18	$5 \cdot 13 \cdot 37 \cdot 109$
524287	19	$3 \cdot 174763$
$3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41$	20	$17 \cdot 61681$
$7^2 \cdot 127 \cdot 337$	21	$3^2 \cdot 43 \cdot 5419$
$3 \cdot 23 \cdot 89 \cdot 683$	22	$5 \cdot 397 \cdot 2113$
$47 \cdot 178481$	23	$3 \cdot 2796203$
$3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$	24	$97 \cdot 257 \cdot 673$
$31 \cdot 601 \cdot 1801$	25	$3 \cdot 11 \cdot 251 \cdot 4051$
$3 \cdot 2731 \cdot 8191$	26	$5 \cdot 53 \cdot 157 \cdot 1613$
$7 \cdot 73 \cdot 262657$	27	$3^4 \cdot 19 \cdot 87211$
$3 \cdot 5 \cdot 29 \cdot 43 \cdot 113 \cdot 127$	28	$17 \cdot 15790321$
$233 \cdot 1103 \cdot 2089$	29	$3 \cdot 59 \cdot 3033169$
$3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$	30	$5^2 \cdot 13 \cdot 41 \cdot 61 \cdot 1321$
2147483647	31	$3 \cdot 715827883$
$3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$	32	$641 \cdot 6700417$
$7 \cdot 23 \cdot 89 \cdot 599479$	33	$3^2 \cdot 67 \cdot 683 \cdot 20857$
$3 \cdot 43691 \cdot 131071$	34	$5 \cdot 137 \cdot 953 \cdot 26317$
$31 \cdot 71 \cdot 127 \cdot 122921$	35	$3 \cdot 11 \cdot 43 \cdot 281 \cdot 86171$
$3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73 \cdot 109$	36	$17 \cdot 241 \cdot 433 \cdot 38737$
$223 \cdot 616318177$	37	$3 \cdot 1777 \cdot 25781083$
$3 \cdot 174763 \cdot 524287$	38	$5 \cdot 229 \cdot 457 \cdot 525313$
$7 \cdot 79 \cdot 8191 \cdot 121369$	39	$3^2 \cdot 2731 \cdot 22366891$
$3 \cdot 5^2 \cdot 11 \cdot 17 \cdot 31 \cdot 41 \cdot 61681$	40	$257 \cdot 4278255361$
$13367 \cdot 164511353$	41	$3 \cdot 83 \cdot 8831418697$
$3^2 \cdot 7^2 \cdot 43 \cdot 127 \cdot 337 \cdot 5419$	42	$5 \cdot 13 \cdot 29 \cdot 113 \cdot 1429 \cdot 14449$
$431 \cdot 9719 \cdot 2099863$	43	$3 \cdot 2932031007403$
$3 \cdot 5 \cdot 23 \cdot 89 \cdot 397 \cdot 683 \cdot 2113$	44	$17 \cdot 353 \cdot 2931542417$
$7 \cdot 31 \cdot 73 \cdot 151 \cdot 631 \cdot 23311$	45	$3^3 \cdot 11 \cdot 19 \cdot 331 \cdot 18837001$
$3 \cdot 47 \cdot 178481 \cdot 2796203$	46	$5 \cdot 277 \cdot 1013 \cdot 1657 \cdot 30269$
$2351 \cdot 4513 \cdot 13264529$	47	$3 \cdot 283 \cdot 165768537521$
$3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 97 \cdot 241 \cdot 257 \cdot 673$	48	$193 \cdot 65537 \cdot 22253377$
$179951 \cdot 3203431780337$	59	$3 \cdot 2833 \cdot 37171 \cdot 1824726041$
$3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$	60	$17 \cdot 241 \cdot 61681 \cdot 4562284561$
$7^2 \cdot 73 \cdot 127 \cdot 337 \cdot 92737 \cdot 649657$	63	$3^3 \cdot 19 \cdot 43 \cdot 5419 \cdot 77158673929$
$3 \cdot 5 \cdot 17 \cdot 257 \cdot 641 \cdot 65537 \cdot 6700417$	64	$274177 \cdot 67280421310721$

$10^e - 1$	e	$10^e + 1$
$3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	6	$101 \cdot 9901$
$3^2 \cdot 239 \cdot 4649$	7	$11 \cdot 909091$
$3^2 \cdot 11 \cdot 73 \cdot 101 \cdot 137$	8	$17 \cdot 5882353$
$3^4 \cdot 37 \cdot 333667$	9	$7 \cdot 11 \cdot 13 \cdot 19 \cdot 52579$
$3^2 \cdot 11 \cdot 41 \cdot 271 \cdot 9091$	10	$101 \cdot 3541 \cdot 27961$
$3^2 \cdot 21649 \cdot 513239$	11	$11^2 \cdot 23 \cdot 4093 \cdot 8779$
$3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 101 \cdot 9901$	12	$73 \cdot 137 \cdot 99990001$
$3^2 \cdot 11 \cdot 17 \cdot 73 \cdot 101 \cdot 137 \cdot 5882353$	16	$353 \cdot 449 \cdot 641 \cdot 1409 \cdot 69857$

числами $Y_n = X_n \bmod 2^4$. Суть выражения (4) состоит в том, что младшие четыре разряда $\langle X_n \rangle$ формируют конгруэнтную последовательность с периодом 16 или меньше. Аналогично пять младших разрядов являются периодичными с периодом не более 32 и наименьший значащий разряд X_n является либо постоянным, либо строго периодичным.

Подобная ситуация не возникает, когда $m = w \pm 1$; в таком случае младшие разряды X_n ведут себя так же случайно, как и старшие. Например, при $w = 2^{35}$ и $m = 2^{35} - 1$ числа последовательности будут не очень случайны, если рассмотреть только их остатки по модулю 31, 71, 127 или 122921 (см. табл. 1); но младшие разряды, которые представляют числа последовательности, взятые по mod 2, будут достаточно случайны.

Альтернатива состоит в том, чтобы в качестве m взять наибольшее простое число, меньше, чем w. Это простое число можно найти, используя методы из раздела 4.5.4 и таблицы из того же раздела, в которых содержатся подходящие большие простые числа.

В большинстве случаев применения младшие разряды несущественны и выбор $m = w$ является совершенно удовлетворительным при условии, что программист, работающий со случайными числами, делает это сознательно.

Обсуждение до сих пор базировалось на использующих "величины со знаками" компьютерах типа MIX. Подобные идеи применяются в вычислительных машинах с дополнительной системой обозначений, хотя есть несколько полезных разновидностей. Например, компьютер DECsystem 20 имеет 36 бит с двоичным арифметическим дополнением; когда он вычисляет произведение двух неотрицательных чисел, младшие разряды содержат 35 бит со знаком "плюс". На этой вычислительной машине следовало бы полагать, что $w = 2^{35}$, но не 2^{36}. 32-битовое двоичное арифметическое дополнение на компьютерах IBM System/370 другое: младшие разряды операции умножения содержат 32 полных бита. Некоторые программисты считают, что это недостаток, так как младшие разряды могут быть отрицательными, когда исходное число положительно, и досадно корректировать это. На самом деле есть определенные *преимущества* с точки зрения генерирования случайных чисел, так как можно брать $m = 2^{32}$ вместо 2^{31} (см. упр. 4).

УПРАЖНЕНИЯ

1. [*M12*] В упр. 3.2.1–3 сделан вывод о том, что наилучший конгруэнтный генератор будет иметь множитель a, взаимно простой с m. Покажите, что, когда $m = w$, возможно лучшее вычисление $(aX + c) \bmod w$ точно в *трех* операциях MIX, чем в четырех операциях (1), с результатом, появляющимся в регистре X.

2. [*16*] Напишите подпрограмму на MIX, имеющую следующие характеристики.

Вызывающая последовательность:	`JMP RANDM`
Условия на входе:	Адрес ячейки `XRAND` содержит целое X
Условия на выходе:	$X \leftarrow \mathrm{rA} \leftarrow (aX + c) \bmod w$, $\mathrm{rX} \leftarrow 0$, переполнение выключено

(В результате обращения к этой подпрограмме можно получить следующее случайное число линейной конгруэнтной последовательности.)

▸ **3.** [*M25*] Многие компьютеры не имеют возможности делить числа из двух слов на числа из одного слова; они позволяют выполнять только операции над числами, из отдельных слов, такие как операция himult — himult $(x, y) = \lfloor xy/w \rfloor$ и операция lomult — lomult $(x, y) = xy \bmod w$, когда x и y — неотрицательные целые числа, меньшие, чем компьютерное слово w. Объясните, как вычислить $ax \bmod m$ в терминах himult и lomult, предполагая, что $0 \le a, x < m < w$ и $m \perp w$. Вы можете использовать заранее вычисленные константы, которые зависят от a, m и w.

▸ **4.** [*21*] Исследуйте вычисление линейной конгруэнтной последовательности с $m = 2^{32}$ на машинах с двоичным дополнением, таких, как компьютеры серии System/370.

5. [*20*] Дано, что m меньше, чем длина слова, и что x и y — неотрицательные целые числа, меньшие, чем m. Покажите, что разность $(x - y) \bmod m$ может быть вычислена точно четырьмя операциями без операции деления на машине MIX. Какая программа будет наилучшей для вычисления суммы $(x + y) \bmod m$?

▸ **6.** [*20*] Предыдущее упражнение наводит на мысль, что вычитание по модулю m — более простая операция, чем суммирование по модулю m. Обсудите последовательность, генерируемую по правилу

$$X_{n+1} = (aX_n - c) \bmod m.$$

Будет ли эта последовательность существенно отличаться от линейной конгруэнтной последовательности, определенной ранее? Будет ли она более эффективной при вычислениях?

7. [*M24*] Какие особенности можно заметить в табл. 1?

▸ **8.** [*20*] Напишите программу для вычисления $(aX) \bmod (w - 1)$ на компьютере MIX, аналогичную программе (2). Значения 0 и $w-1$ на входе и выходе вашей программы считаются эквивалентными.

▸ **9.** [*M25*] В большинстве языков программирования высокого уровня не предусмотрен хороший способ деления целого числа из двух слов на целое число из одного слова. Не предусматривается это и операцией himult из упр. 3. Цель данного упражнения — найти приемлемый способ преодоления таких ограничений, когда необходимо вычислить $ax \bmod m$ для переменной x и константы $0 < a < m$.

a) Докажите, что если $q = \lfloor m/a \rfloor$, то $a(x - (x \bmod q)) = \lfloor x/q \rfloor (m - (m \bmod a))$.

b) С помощью равенства (a) вычислите $ax \bmod m$, не оперируя числами, которые превосходят m по абсолютной величине, и предполагая, что $a^2 \le m$.

10. [*M26*] Решение упр. 9, (b) иногда применимо, когда $a^2 > m$. Определите точное число множителей a, для которых промежуточные результаты этого метода никогда не превосходят m для всех x между 0 и m.

11. [*M30*] Продолжая упр. 9, покажите, что можно оценить $ax \bmod m$, используя только следующие основные операции:

i) $u \times v$, где $u \ge 0$, $v \ge 0$ и $uv < m$;
ii) $\lfloor u/v \rfloor$, где $0 < v \le u < m$;
iii) $(u - v) \bmod m$, где $0 \le u, v < m$.

Действительно, это всегда возможно, если использовать максимум 12 операций типа (i) и (ii) и ограниченное число операций типа (iii), не считая предварительного вычисления констант, которые зависят от a и m. Например, объясните, как можно выполнить вычисления, когда a равно 62089911 и m равно $2^{31} - 1$. (Эти константы взяты из табл. 3.3.4–1.)

▸ **12.** [*M28*] Рассмотрите вычисления карандашом на бумаге или на счетах.

a) Найдите хороший метод умножения заданного десятизначного числа на 10 по модулю 9999998999.

b) Сделайте то же самое, но умножив не на 10, а на 999999900 (по модулю 9999998999).

c) Объясните, как вычислить степень $999999900^n \bmod 9999998999$ для $n = 1,2,3,\ldots$.

d) Выполните такие же вычисления с десятичным разложением числа $1/9999998999$.

e) Покажите, что эти идеи предоставляют возможность реализовать определенные виды линейных конгруэнтных генераторов, имеющих очень большие модули, с помощью лишь нескольких операций с генерируемым числом.

13. [*M24*] Повторите предыдущее упражнение, но с модулем 9999999001 и множителями 10 и 8999999101.

14. [*M25*] Обобщите идеи предыдущих двух упражнений для того, чтобы получить большое семейство линейных конгруэнтных генераторов с особенно большими модулями.

3.2.1.2. Выбор множителя. В этом разделе будут рассмотрены методы выбора множителя a для создания *периода максимальной длины*. Длинный период необходим для любой последовательности, используемой в качестве источника случайных чисел. Безусловно, мы ожидаем, что в периоде содержится значительно больше чисел, чем требуется для одноразового использования. Поэтому здесь внимание будет сосредоточено на длине периода. Читателю следовало бы помнить, однако, что длина периода — это только одно из требований к линейным конгруэнтным последовательностям, которые мы хотим использовать, как случайные последовательности. Например, когда $a = c = 1$, последовательность примет простой вид: $X_{n+1} = (X_n + 1) \bmod m$. Она, очевидно, имеет период длиной m, но несмотря на это в ней нет ничего случайного. Другие соображения, влияющие на выбор множителя, будут приведены ниже в этой главе. Так как возможны только m различных значений, длина периода, несомненно, не может быть больше m. Можно ли достичь максимальной длины периода — m? Пример, приведенный выше, показывает, что это всегда возможно, хотя выбор $a = c = 1$ не обеспечивает желаемые свойства последовательности. Исследуем *все* возможные значения a, c и X_0, которые дают период длиной m. Оказывается, что такие значения параметров могут быть охарактеризованы очень просто; когда m является произведением различных простых чисел, только значение $a = 1$ обеспечивает полный период, но когда m делится на простое число в большой степени, то существует значительная свобода в выборе a. Следующая теорема позволяет легко определить, возможно ли достижение периода максимальной длины.

Теорема A. *Линейная конгруэнтная последовательность, определенная числами m, a, c и X_0, имеет период длиной m тогда и только тогда, когда:*

i) *числа c и m взаимно простые;*

ii) *$b = a - 1$ кратно p для каждого простого p, являющегося делителем m;*

iii) *b кратно 4, если m кратно 4.*

Идеи, используемые при доказательстве этой теоремы, впервые возникли, по крайней мере, сто лет тому назад. Но первое ее доказательство в этой особой форме было предложено М. Гринбергером (M. Greenberger) для частного случая при $m = 2^e$ [см. *JACM* **8** (1961), 383–389]. Достаточность условий (i)–(iii) в общем случае была доказана Халлом (Hull) и Добеллом (Dobell) [см. *SIAM Review* **4**

(1962), 230–254]. Чтобы доказать теорему, мы сначала рассмотрим некоторые вспомогательные теоретико-числовые результаты, представляющие и самостоятельный интерес.

Лемма P. *Пусть p — простое число, а e — положительное целое число, такое, что $p^e > 2$. Если*

$$x \equiv 1 \text{ (по модулю } p^e), \qquad x \not\equiv 1 \text{ (по модулю } p^{e+1}), \tag{1}$$

то

$$x^p \equiv 1 \text{ (по модулю } p^{e+1}), \qquad x^p \not\equiv 1 \text{ (по модулю } p^{e+2}). \tag{2}$$

Доказательство. Если x не кратно p, то оно может быть представлено в виде $x = 1 + qp^e$ для некоторого целого q. По биномиальной формуле получаем

$$\begin{aligned} x^p &= 1 + \binom{p}{1} qp^e + \cdots + \binom{p}{p-1} q^{p-1} p^{(p-1)e} + q^p p^{pe} \\ &= 1 + qp^{e+1} \left(1 + \frac{1}{p}\binom{p}{2} qp^e + \frac{1}{p}\binom{p}{3} q^2 p^{2e} + \cdots + \frac{1}{p}\binom{p}{p} q^{p-1} p^{(p-1)e} \right) \end{aligned}$$

Величины в скобках являются целыми числами, и к тому же каждый член внутри скобок, за исключением первого, кратен p. Для таких k, что $1 < k < p$, биномиальные коэффициенты $\binom{p}{k}$ делятся на p (см. упр. 1.2.6–10); следовательно,

$$\frac{1}{p}\binom{p}{k} q^{k-1} p^{(k-1)e}$$

делится на $p^{(k-1)e}$. Последний член $q^{p-1}p^{(p-1)e-1}$ также делится на p, поскольку $(p-1)e > 1$, когда $p^e > 2$. Итак, $x^p \equiv 1 + qp^{e+1}$ (по модулю p^{e+2}), что и завершает доказательство. (*Замечание.* Обобщение этого результата приведено в упр. 3.2.2–11, (a).) ∎

Лемма Q. *Пусть число m допускает разложение на простые множители в виде*

$$m = p_1^{e_1} \ldots p_t^{e_t}. \tag{3}$$

Длина периода λ линейной конгруэнтной последовательности, определенной параметрами (X_0, a, c, m), является наименьшим общим кратным длин λ_j периодов линейных конгруэнтных последовательностей $(X_0 \bmod p_j^{e_j}, a \bmod p_j^{e_j}, c \bmod p_j^{e_j}, p_j^{e_j})$, $1 \le j \le t$.

Доказательство. Если использовать индукцию по t, то достаточно доказать, что если m_1 и m_2 — взаимно простые числа, то длина λ линейной конгруэнтной последовательности, определенной параметрами $(X_0, a, c, m_1 m_2)$, является наименьшим общим кратным длин λ_1 и λ_2 периодов последовательностей, определенных параметрами $(X_0 \bmod m_1, a \bmod m_1, c \bmod m_1, m_1)$ и $(X_0 \bmod m_2, a \bmod m_2, c \bmod m_2, m_2)$. В предыдущем разделе мы заметили (см. (4)), что если элементы этих трех последовательностей соответственно обозначены через X_n, Y_n и Z_n, то справедливо равенство

$$Y_n = X_n \bmod m_1 \qquad \text{и} \qquad Z_n = X_n \bmod m_2 \qquad \text{для всех } n \ge 0.$$

Поэтому по закону D из раздела 1.2.4 находим, что

$$X_n = X_k \qquad \text{тогда и только тогда, когда} \qquad Y_n = Y_k \quad \text{и} \quad Z_n = Z_k. \tag{4}$$

Пусть λ' — наименьшее общее кратное λ_1 и λ_2. Необходимо доказать, что $\lambda' = \lambda$. Так как $X_n = X_{n+\lambda}$ для всех достаточно больших n, $Y_n = Y_{n+\lambda}$ (следовательно, λ кратно λ_1) и $Z_n = Z_{n+\lambda}$ (следовательно, λ кратно λ_2). Таким образом, получим, что $\lambda \geq \lambda'$. Более того, известно, что $Y_n = Y_{n+\lambda'}$ и $Z_n = Z_{n+\lambda'}$ для всех достаточно больших n; поэтому из (4) следует, что $X_n = X_{n+\lambda'}$. Это доказывает, что $\lambda \leq \lambda'$. ▮

Сейчас мы готовы доказать теорему A. Из леммы Q следует, что теорему достаточно доказать для случая, когда m является степенью простого числа, поскольку

$$p_1^{e_1} \ldots p_t^{e_t} = \lambda = \operatorname{lcm}(\lambda_1, \ldots, \lambda_t) \leq \lambda_1 \ldots \lambda_t \leq p_1^{e_1} \ldots p_t^{e_t}$$

(lcm — наименьшее общее кратное. — *Прим. перев.*) выполняется тогда и только тогда, когда $\lambda_j = p_j^{e_j}$ для $1 \leq j \leq t$.

Предположим поэтому, что $m = p^e$, где p — простое число, а e — целое положительное число. Поскольку утверждение теоремы очевидно при $a = 1$, можно считать, что $a > 1$. Период может иметь длину m тогда и только тогда, когда каждое целое число x, такое, что $0 \leq x < m$, встречается в этом периоде. Действительно, никакое значение x в периоде не может встретиться более одного раза. Таким образом, период имеет длину m тогда и только тогда, когда период последовательности с начальным значением $X_0 = 0$ имеет период длиной m. Поэтому достаточно доказать теорему, когда $X_0 = 0$. Из формулы 3.2.1–(6) следует, что

$$X_n = \left(\frac{a^n - 1}{a - 1}\right) c \bmod m. \tag{5}$$

Если c и m не взаимно простые числа, то значение X_n никогда не может быть равно 1. Следовательно, условие (i) теоремы необходимо. Период имеет длину m тогда и только тогда, когда наименьшее положительное значение n, для которого $X_n = X_0 = 0$, равняется $n = m$. Из (5) и условия (i) следует, что доказательство нашей теоремы сводится к доказательству следующего утверждения.

Лемма R. *Предположим, что $1 < a < p^e$, где p — простое число. Если λ — наименьшее целое положительное число, для которого $(a^\lambda - 1)/(a - 1) \equiv 0$ (по модулю p^e), то*

$$\lambda = p^e \quad \textit{тогда и только тогда, когда} \quad \begin{cases} a \equiv 1 \text{ (по модулю } p), & \textit{где} \quad p > 2, \\ a \equiv 1 \text{ (по модулю } 4), & \textit{где} \quad p = 2. \end{cases}$$

Доказательство. Предположим, что $\lambda = p^e$. Если $a \not\equiv 1$ (по модулю p), то $(a^n - 1)/(a - 1) \equiv 0$ (по модулю p^e) тогда и только тогда, когда $a^n - 1 \equiv 0$ (по модулю p^e). Значит, условие $a^{p^e} - 1 \equiv 0$ (по модулю p^e) влечет равенство $a^{p^e} \equiv 1$ (по модулю p), но из теоремы 1.2.4F следует, что $a^{p^e} \equiv a$ (по модулю p). Таким образом, предположение, что $a \not\equiv 1$ (по модулю p), приводит к противоречию. Если $p = 2$ и $a \equiv 3$ (по модулю 4), то из упр. 8 следует

$$(a^{2^{e-1}} - 1)/(a - 1) \equiv 0 \text{ (по модулю } 2^e).$$

Эти рассуждения показывают, что в большинстве случаев необходимо, чтобы $a = 1 + qp^f$, где $p^f > 2$ и q не кратны p, всякий раз, когда $\lambda = p^e$.

Остается показать, что это условие *достаточно* для того, чтобы $\lambda = p^e$. Применив лемму P, находим, что для всех $g \geq 0$

$$a^{p^g} \equiv 1 \text{ (по модулю } p^{f+g}), \qquad a^{p^g} \not\equiv 1 \text{ (по модулю } p^{f+g+1});$$

следовательно,

$$\begin{aligned} (a^{p^g} - 1)/(a-1) &\equiv 0 \text{ (по модулю } p^g), \\ (a^{p^g} - 1)/(a-1) &\not\equiv 0 \text{ (по модулю } p^{g+1}). \end{aligned} \tag{6}$$

В частности, $(a^{p^e} - 1)/(a-1) \equiv 0$ (по модулю p^e). Сейчас для конгруэнтной последовательности, определяемой параметрами $(0, a, 1, p^e)$ X_n, справедливо $X_n = (a^n - 1)/(a-1) \bmod p^e$. Значит, ее период равен λ, т. е. $X_n = 0$ тогда и только тогда, когда n кратно λ. Следовательно, p^e кратно λ. Это может случиться, только если $\lambda = p^g$ для некоторых g и соотношения (6) означают, что $\lambda = p^e$. ▮

Итак, теорема A доказана. ▮

В завершение этого раздела рассмотрим специальный случай использования исключительно мультипликативных генераторов, когда $c = 0$. Несмотря на то что процесс генерирования случайных чисел является немного более быстрым в данном случае, теорема A показывает, что максимальный период не может быть достигнут. Действительно, это совершенно очевидно, так как последовательность удовлетворяет соотношению

$$X_{n+1} = aX_n \bmod m \tag{7}$$

и значение $X_n = 0$ может появиться, только если последовательность вырождается в нуль. Вообще, если d — любой делитель m и если X_n кратно d, все последующие элементы мультипликативной последовательности $X_{n+1}, X_{n+2}, \ldots$ будут кратны d. Так что когда $c = 0$, необходимо, чтобы X_n и m были взаимно простыми числами для всех n, что и ограничивает длину периода максимум до $\varphi(m)$ — числа целых взаимно простых чисел с m, лежащих между 0 и m.

Приемлемой длины периода можно достичь, даже если оговорить, что $c = 0$. Давайте сейчас попытаемся найти такие условия, которым удовлетворяет множитель, чтобы в этом специальном случае период стал настолько длинным, насколько это возможно.

Согласно лемме Q период последовательности зависит исключительно от периодов последовательностей при $m = p^e$. Рассмотрим эту ситуацию. Итак, $X_n = a^n X_0 \bmod p^e$ и ясно, что период будет иметь длину 1 (здесь можно только сказать, что длина периода не больше, чем e. — *Прим. ред.*), если a кратно p. Поэтому будем считать, что a и p взаимно простые. Тогда период будет наименьшим целым числом λ, таким, что $X_0 = a^\lambda X_0 \bmod p^e$. Если наибольшим общим делителем X_0 и p^e является p^f, то это условие эквивалентно условию

$$a^\lambda \equiv 1 \text{ (по модулю } p^{e-f}). \tag{8}$$

По теореме Эйлера (упр. 1.2.4–28) $a^{\varphi(p^{e-f})} \equiv 1$ (по модулю p^{e-f}); следовательно, λ является делителем

$$\varphi(p^{e-f}) = p^{e-f-1}(p-1).$$

Когда a и m — взаимно простые числа, наименьшее число λ, для которого $a^\lambda \equiv 1$ (по модулю m), принято называть *порядком a по модулю m*. Любое такое значение a, которое имеет *максимальный* возможный порядок по модулю m, называют *первообразным элементом* по модулю m.

Обозначим через $\lambda(m)$ порядок первообразного элемента, а именно — максимальный возможный порядок по модулю m. Из замечаний следует, что $\lambda(p^e)$ является делителем $p^{e-1}(p-1)$; достаточно легко (см. упр. 11–16, приведенные ниже) можно определить значения $\lambda(m)$ во всех следующих случаях:

$$\begin{aligned} \lambda(2) = 1, \qquad \lambda(4) = 2, \qquad \lambda(2^e) = 2^{e-2}, \quad \text{если} \quad e \ge 3; \\ \lambda(p^e) = p^{e-1}(p-1), \qquad \text{если} \quad p > 2; \\ \lambda(p_1^{e_1} \ldots p_t^{e_t}) = \operatorname{lcm}\big(\lambda(p_1^{e_1}), \ldots, \lambda(p_t^{e_t})\big). \end{aligned} \tag{9}$$

Все сказанное можно подытожить в следующей теореме.

Теорема B. [C. F. Gauss, *Disquisitiones Arithmeticæ* (1801), §90–92.] *Максимальным периодом, возможным, когда $c = 0$, является $\lambda(m)$, где $\lambda(m)$ определено в* (9). *Этот период достигается, если:*

i) *X_0 и m — взаимно простые числа;*

ii) *a является первообразным элементом по модулю m.* ▮

Заметим, что можно получить период длиной $m - 1$, если m — простое число; т. е. это всего на единицу меньше, чем максимальная длина периода. Так что для практических целей такой период может быть настолько длинным, насколько это необходимо.

Теперь возникает вопрос, как найти первообразные элементы по модулю m? В упражнениях, данных в конце раздела, приводится совершенно очевидный ответ на вопрос, когда m является простым числом или степенью простого числа. Результаты сформулированы в следующей теореме.

Теорема C. *Число a является первообразным элементом по модулю p^e тогда и только тогда, когда выполняется одно из следующих условий:*

i) *$p = 2$, $e = 1$ и a — нечетное число;*

ii) *$p = 2$, $e = 2$ и $a \bmod 4 = 3$;*

iii) *$p = 2$, $e = 3$ и $a \bmod 8 = 3$, 5 или 7;*

iv) *$p = 2$, $e \ge 4$ и $a \bmod 8 = 3$ или 5;*

v) *p — нечетное число, $e = 1$, $a \not\equiv 0$ (по модулю p) и $a^{(p-1)/q} \not\equiv 1$ (по модулю p) для любого простого делителя q числа $p - 1$;*

vi) *p — нечетное число, $e > 1$, a удовлетворяют условию* (v) *и $a^{p-1} \not\equiv 1$* (по модулю p^2). ▮

Условия (v) и (vi) теоремы легко проверяются на компьютере для больших p. Эффективные методы оценки степени, когда известны множители числа $p - 1$, обсуждаются в разделе 4.6.3.

Теорема C применима только к степеням простых чисел. Но если заданы значения a_j, являющиеся первообразными элементами по модулю $p_j^{e_j}$, то можно найти

единственное значение a, такое, что $a \equiv a_j$ (по модулю $p_j^{e_j}$) при $1 \le j \le t$, используя китайский алгоритм (алгоритм, построенный на основании китайской теоремы об остатках. — *Прим. перев.*), рассматриваемый в разделе 4.3.2. Число a будет первообразным элементом по модулю $p_1^{e_1} \ldots p_t^{e_t}$. Таким образом, существует приемлемый эффективный путь построения множителей, удовлетворяющих условию теоремы B, для любых модулей m умеренной размерности, хотя вычисления в общем случае могут быть весьма длинными.

В распространенном случае, когда $m = 2^e$, где $e \ge 4$, изложенные выше условия приводят к единственному требованию: $a \equiv 3$ или 5 (по модулю 8). В этой ситуации четвертая часть всех возможных множителей даст длину периода, равную $m/4$, а $m/4$ будет максимальной длиной периода, когда $c = 0$.

Существует второй, еще более распространенный случай, когда $m = 10^e$. Используя леммы P и Q, нетрудно получить необходимые и достаточные условия достижения максимального периода для десятичного компьютера (см. упр. 18).

Теорема D. *Если* $m = 10^e$, $e \ge 5$, $c = 0$ *и* X_0 *не кратно* 2 *или* 5, *то период линейной конгруэнтной последовательности равен* $5 \times 10^{e-2}$ *тогда и только тогда, когда* $a \bmod 200$ *равно одному из следующих* 32 *чисел:*

$$\begin{array}{l} 3,\ 11,\ 13,\ 19,\ 21,\ 27,\ 29,\ 37,\ 53,\ 59,\ 61,\ 67,\ 69,\ 77,\ 83,\ 91,\ 109,\ 117,\\ 123,\ 131,\ 133,\ 139,\ 141,\ 147,\ 163,\ 171,\ 173,\ 179,\ 181,\ 187,\ 189,\ 197. \quad \blacksquare \end{array} \tag{10}$$

УПРАЖНЕНИЯ

1. [*10*] Чему равна длина периода линейной конгруэнтной последовательности с параметрами $X_0 = 5772156648$, $a = 3141592621$, $c = 2718281829$ и $m = 10000000000$?

2. [*10*] Будут ли следующие два условия гарантировать максимальную длину периода, когда m является степенью 2? (i) c — нечетное число; (ii) $a \bmod 4 = 1$.

3. [*13*] Предположим, что $m = 10^e$, где $e \ge 2$, и пусть c — нечетное число, не кратное 5. Покажите, что линейная конгруэнтная последовательность будет иметь период максимальной длины тогда и только тогда, когда $a \bmod 20 = 1$.

4. [*M20*] Предположим, что $m = 2^e$ и $X_0 = 0$. Если числа a и c удовлетворяют условиям теоремы A, чему равно $X_{2^{e-1}}$?

5. [*14*] Найдите все множители a, удовлетворяющие условиям теоремы A, когда $m = 2^{35} + 1$. (Простые множители m можно найти в табл. 3.2.1.1–1.)

▸ **6.** [*20*] Найдите все множители a, удовлетворяющие условиям теоремы A, когда $m = 10^6 - 1$ (см. табл. 3.2.1.1–1).

▸ **7.** [*M23*] Период конгруэнтной последовательности не должен начинаться с X_0, но всегда можно найти индексы $\mu \ge 0$ и $\lambda > 0$, такие, что $X_{n+\lambda} = X_n$ при всех $n \ge \mu$, и для которых μ и λ являются наименьшими возможными значениями с этими свойствами (см. упр. 3.1–6 и 3.2.1–1). Если μ_j и λ_j — индексы, соответствующие последовательностям

$$(X_0 \bmod p_j^{e_j},\ a \bmod p_j^{e_j},\ c \bmod p_j^{e_j},\ p_j^{e_j}),$$

и если μ и λ соответствуют составной последовательности $(X_0, a, c, p_1^{e_1} \ldots p_t^{e_t})$, то согласно формулировке леммы Q λ является наименьшим общим кратным $\lambda_1, \ldots, \lambda_t$. Чему равно значение μ в терминах значений $\mu_1, \ldots, \mu_t$? Чему равно максимально возможное значение μ, получаемое путем варьирования X_0, a и c, когда $m = p_1^{e_1} \ldots p_t^{e_t}$ фиксировано?

8. [*M20*] Покажите, что если $a \bmod 4 = 3$, то $(a^{2^{e-1}} - 1)/(a - 1) \equiv 0$ (по модулю 2^e), когда $e > 1$. (Воспользуйтесь леммой P.)

▸ **9.** [*M22*] (В. Э. Томсон (W. E. Thomson).) Когда $c = 0$ и $m = 2^e \geq 16$, теоремы B и C утверждают, что период имеет длину 2^{e-2} тогда и только тогда, когда множитель a удовлетворяет равенствам $a \bmod 8 = 3$ или $a \bmod 8 = 5$. Покажите, что каждая такая последовательность, по существу, является линейной конгруэнтной последовательностью с $m = 2^{e-2}$, имеющей *полный* период, в следующем смысле:

a) если $X_{n+1} = (4c+1)X_n \bmod 2^e$ и $X_n = 4Y_n + 1$, то

$$Y_{n+1} = ((4c+1)Y_n + c) \bmod 2^{e-2};$$

b) если $X_{n+1} = (4c-1)X_n \bmod 2^e$ и $X_n = ((-1)^n(4Y_n+1)) \bmod 2^e$, то

$$Y_{n+1} = ((1-4c)Y_n - c) \bmod 2^{e-2}$$

[*Замечание.* В этих формулах c есть нечетное целое число. В литературе содержится достаточно утверждений о том, что последовательности с $c = 0$, удовлетворяющие теореме B, так или иначе являются более случайными, чем последовательности, удовлетворяющие условиям теоремы A, вопреки тому факту, что период — это только четверть длины периода, получаемого в условиях теоремы B. В данном упражнении такие утверждения опровергаются; в сущности, следует удалить два разряда длины слова, чтобы сохранить возможность прибавить c, когда m будет степенью 2.]

10. [*M21*] Для каких значений m справедливо $\lambda(m) = \varphi(m)$?

▸ **11.** [*M28*] Пусть x — нечетное целое число, большее, чем 1. (a) Покажите, что существует единственное целое число $f > 1$, такое, что $x \equiv 2^f \pm 1$ (по модулю 2^{f+1}). (b) Дано, что $1 < x < 2^e - 1$ и что f является соответствующим целым числом п. (a). Покажите, что порядок x по модулю 2^e равен 2^{e-f}. (c) В частности, это доказывает утверждения (i)–(iv) теоремы C.

12. [*M26*] Пусть p — простое нечетное число. Если $e > 1$, докажите, что a является первообразным элементом по модулю p^e тогда и только тогда, когда a — первообразный элемент по модулю p и $a^{p-1} \not\equiv 1$ (по модулю p^2). (Предположите, что $\lambda(p^e) = p^{e-1}(p-1)$. Этот факт доказан в упр. 14 и 16 ниже.)

13. [*M22*] Пусть p — простое число. Задано, что a не является первообразным элементом по модулю p. Покажите, что каждое a кратно p или $a^{(p-1)/q} \equiv 1$ (по модулю p) для некоторых простых чисел q, делящих $p-1$.

14. [*M18*] Предположим, что $e > 1$, p — нечетное простое число и a — первообразный элемент по модулю p. Докажите, что либо a, либо $a+p$ является первообразным элементом по модулю p^e. [*Указание.* См. упр. 12.]

15. [*M29*] (a) Пусть a_1 и a_2 взаимно просты с m и пусть их порядки по модулю m равны соответственно λ_1 и λ_2. Предположим, что λ является наименьшим общим кратным λ_1 и λ_2. Докажите, что $a_1^{\kappa_1}a_2^{\kappa_2}$ имеют порядок λ по модулю m для соответствующих целых чисел κ_1 и κ_2. [*Указание.* Рассмотрите сначала случай, когда λ_1 и λ_2 — взаимно простые числа.] (b) Пусть $\lambda(m)$ — максимальный порядок любого элемента по модулю m. Докажите, что $\lambda(m)$ кратно порядку каждого элемента по модулю m, т. е. что $a^{\lambda(m)} \equiv 1$ (по модулю m) всегда, когда a и m — взаимно простые числа. (Не используйте теорему B.)

▸ **16.** [*M24*] (*Существование первообразных корней.*) Пусть p — простое число.

a) Рассмотрим полином $f(x) = x^n + c_1x^{n-1} + \cdots + c_n$, где c_i — целые числа. Дано, что a — целое число, для которого $f(a) \equiv 0$ (по модулю p). Покажите, что существует полином

$$q(x) = x^{n-1} + q_1x^{n-2} + \cdots + q_{n-1}$$

с целыми коэффициентами, такой, что $f(x) \equiv (x-a)q(x)$ (по модулю p) для всех целых x.

b) Пусть $f(x)$ — такой же полином, как в (a). Покажите, что $f(x)$ имеет не более n различных "корней" по модулю p, т. е. существует не более n целых чисел a, $0 \le a < p$, таких, что $f(a) \equiv 0$ (по модулю p).

c) Так же, как и в упр. 15, (b), полином $f(x) = x^{\lambda(p)} - 1$ имеет $p - 1$ различных корней; следовательно, существует целое число a с порядком $p - 1$.

17. [*M26*] Не все значения, перечисленные в теореме D, можно получить, используя построения, приведенные в разделе, например 11 — не первообразный элемент по модулю 5^e. Как это возможно, если 11 *является* первообразным элементом по модулю 10^e согласно теореме D? Какие из чисел, перечисленных в теореме D, являются *одновременно* первообразными элементами по модулям 2^e и 5^e?

18. [*M25*] Докажите теорему D (см. предыдущее упражнение).

19. [*40*] Составьте таблицу нескольких подходящих множителей a для каждого из значений m, внесенных в табл. 3.2.1.1–1, предполагая, что $c = 0$.

▸ **20.** [*M24*] (Дж. Марсалья (G. Marsaglia).) Назначение упражнения состоит в изучении длины периода *произвольной* линейной конгруэнтной последовательности. Пусть $Y_n = 1 + a + \cdots + a^{n-1}$, так что $X_n = (AY_n + X_0) \bmod m$ для некоторой константы A из условия 3.2.1–(8).

a) Докажите, что длина периода $\langle X_n \rangle$ равна длине периода $\langle Y_n \bmod m' \rangle$, когда $m' = m/\gcd(A, m)$.

b) Докажите, что длина периода $\langle Y_n \bmod p^e \rangle$ удовлетворяет следующим требованиям, когда p — простое число. (i) Если $a \bmod p = 0$, длина периода равна 1. (ii) Если $a \bmod p = 1$, она равна p^e, за исключением случаев, когда $p = 2$, $e \ge 2$ и $a \bmod 4 = 3$. (iii) Если $p = 2$, $e \ge 2$ и $a \bmod 4 = 3$, она равна удвоенному порядку a по модулю p^e (см. упр. 11), за исключением случая, когда $a \equiv -1$ (по модулю 2^e), при котором она равна 2. (iv) Если $a \bmod p > 1$, длина периода равна порядку a по модулю p^e.

21. [*M25*] Пусть в линейной конгруэнтной последовательности с максимальным периодом $X_0 = 0$ s — наименьшее положительное целое число, такое, что $a^s \equiv 1$ (по модулю m). Докажите, что $\gcd(X_s, m) = s$ (gcd — наибольший общий делитель. — *Прим. перев.*).

▸ **22.** [*M25*] Обсудите проблему нахождения модулей $m = b^k \pm b^l \pm 1$ таким образом, чтобы генераторы, использующие вычитание с заимствованием и суммирование с переносом (см. упр. 3.2.1.1–14), имели очень длинные периоды.

3.2.1.3. Потенциал. В предыдущем разделе было показано, что максимальный период может быть достигнут, когда $b = a - 1$ кратно каждому простому делителю m, и b должно быть также кратно 4, если m кратно 4. Если z — основание системы счисления машины ($z = 2$ для бинарного компьютера и $z = 10$ для десятичного компьютера), m — длина слова в компьютере z^e, множитель

$$a = z^k + 1, \qquad 2 \le k < e, \tag{1}$$

удовлетворяет этим условиям. По теореме 3.2.1.2A можно брать $c = 1$. Рекуррентное соотношение теперь имеет вид

$$X_{n+1} = \big((z^k + 1)X_n + 1\big) \bmod z^e, \tag{2}$$

и это уравнение означает, что можно избежать умножения; просто достаточно перемещения и суммирования.

Например, пусть $a = B^2 + 1$, где B — размер байта компьютера MIX. Программа

```
LDA X;  SLA 2;  ADD X;  INCA 1
```
(3)

может использоваться вместо программы, приведенной в разделе 3.2.1.1, и время выполнения программы уменьшается от $16u$ до $7u$.

По этой причине множители, имеющие вид (1), широко обсуждались в литературе. Они действительно рекомендованы многими авторами. Однако первые несколько лет экспериментирования с этим методом убедительно показали, что *множителей, имеющих простой вид* (1), *следует избегать.* Сгенерированные числа просто недостаточно случайны.

Ниже в этой главе будет рассмотрена одна довольно сложная теория, связанная с недостатками всех известных плохих линейных конгруэнтных генераторов случайных чисел. Однако некоторые генераторы (такие, как (2)) настолько ужасны, что достаточно сравнительно простой теории, чтобы исключить их из рассмотрения. Эта простая теория связана с понятием "потенциал", которое мы сейчас обсудим.

Потенциал линейной конгруэнтной последовательности с максимальным периодом определяется как наименьшее целое число s, такое, что

$$b^s \equiv 0 \ (\text{по модулю } m). \tag{4}$$

(Целое число s всегда существует, когда множитель удовлетворяет условиям теоремы 3.2.1.2A, так как b кратно каждому простому делителю m.)

Можно анализировать случайность последовательности, положив $X_0 = 0$, так как 0 встречается в периоде. При этом предположении соотношение 3.2.1–(6) сводится к

$$X_n = \big((a^n - 1)c/b\big) \bmod m;$$

и, если разложить выражение $a^n - 1 = (b + 1)^n - 1$ по биномиальной формуле, получится

$$X_n = c\left(n + \binom{n}{2} b + \cdots + \binom{n}{s} b^{s-1}\right) \bmod m. \tag{5}$$

Все члены разложения b^s, b^{s+1} и т. д. можно исключить, так как они кратны m.

Уравнение (5) столь поучительно, что необходимо рассмотреть некоторые специальные случаи. Если $a = 1$, потенциал равен 1 и $X_n \equiv cn$ (по модулю m), как мы уже видели, так что последовательность наверняка не случайна. Если потенциал равен 2, то $X_n \equiv cn + cb\binom{n}{2}$, и снова последовательность не совсем случайна. Действительно, в этом случае

$$X_{n+1} - X_n \equiv c + cbn.$$

Таким образом, разность между последовательно генерируемыми числами выражена простой зависимостью от n. Точка (X_n, X_{n+1}, X_{n+2}) всегда лежит на одной из четырех плоскостей в трехмерном пространстве:

$$x - 2y + z = d + m, \qquad x - 2y + z = d - m,$$
$$x - 2y + z = d, \qquad x - 2y + z = d - 2m,$$

где $d = cb \bmod m$.

Если потенциал равен 3, то последовательность становится более или менее похожей на случайную, но все еще существует высокая степень зависимости между X_n, X_{n+1} и X_{n+2}. Тесты показывают, что последовательности с потенциалом 3 попрежнему недостаточно хороши. Сообщалось, что приемлемые результаты были получены в некоторых случаях при потенциале, равном 4, но это оспаривалось

другими исследователями. Кажется, что последовательности с потенциалом 5 и выше обладают достаточно хорошими случайными свойствами.

Предположим, например, что $m = 2^{35}$ и $a = 2^k + 1$. Тогда $b = 2^k$, так что величины $b^2 = 2^{2k}$ кратны m, когда $k \geq 18$: потенциал равен 2. Если $k = 17, 16, \ldots, 12$, то потенциал равен 3 и значение потенциала 4 достигается для $k = 11, 10, 9$. Таким образом, с точки зрения потенциала множители приемлемы при $k \leq 8$. Это означает, что $a \leq 257$, но, как мы увидим позже, *малых* множителей также следует избегать. Итак, все множители вида $2^k + 1$, когда $m = 2^{35}$, исключены.

Когда m равно $w \pm 1$, где w — длина слова компьютера, m, вообще говоря, не делится на высокие степени простых чисел и высокий потенциал невозможен (см. упр. 6). Таким образом, в этом случае *не* следует использовать метод максимального периода; лучше использовать метод чистого умножения со значением $c = 0$.

Нужно подчеркнуть, что высокий потенциал является необходимым, но недостаточным условием случайности; мы использовали понятие потенциала для того, чтобы исключить несостоятельные генераторы, но не для того, чтобы безусловно принимать все генераторы с высоким потенциалом. Линейные конгруэнтные последовательности должны пройти "спектральный тест", обсуждаемый в разделе 3.3.4, прежде чем они будут признаны случайными.

УПРАЖНЕНИЯ

1. [*M10*] Покажите, что независимо от размера байта B компьютера MIX программа (3) генерирует последовательность случайных чисел с максимальным периодом.

2. [*10*] Чему равен потенциал генератора, предложенного в программе (3) для компьютера MIX?

3. [*11*] Чему равен потенциал линейной конгруэнтной последовательности, когда $m = 2^{35}$ и $a = 3141592621$? Чему равен потенциал, если множитель равен $a = 2^{23} + 2^{13} + 2^2 + 1$?

4. [*15*] Покажите, что если $m = 2^e \geq 8$, то максимум потенциала достигается при $a \bmod 8 = 5$.

5. [*M20*] Дано, что $m = p_1^{e_1} \ldots p_t^{e_t}$ и $a = 1 + kp_1^{f_1} \ldots p_t^{f_t}$, где a удовлетворяет условиям теоремы 3.2.1.2A и k и m — взаимно простые числа. Покажите, что потенциал равен $\max(\lceil e_1/f_1 \rceil, \ldots, \lceil e_t/f_t \rceil)$.

▸ **6.** [*20*] Какие значения $m = w \pm 1$ из табл. 3.2.1.1–1 могут быть использованы в линейной конгруэнтной последовательности с максимальным периодом, чтобы ее потенциал был равен 4 или выше? (Воспользуйтесь результатом упр. 5.)

7. [*M20*] Когда a удовлетворяет условиям теоремы 3.2.1.2A, оно взаимно просто с m; поэтому существует число a', такое, что $aa' \equiv 1$ (по модулю m). Покажите, что a' может быть просто записано в терминах b.

▸ **8.** [*M26*] Генератор случайных чисел, определенный как $X_{n+1} = (2^{17} + 3)X_n \bmod 2^{35}$ и $X_0 = 1$, был протестирован следующим образом: пусть $Y_n = \lfloor 10X_n/2^{35} \rfloor$; тогда Y_n должен быть случайной цифрой между 0 и 9 и тройка цифр $(Y_{3n}, Y_{3n+1}, Y_{3n+2})$ должна принимать каждое из 1 000 возможных значений от (0, 0, 0) до (9, 9, 9) с приблизительно равными частотами. Но после того как было проверено 30 000 значений, оказалось, что одни тройки встречались крайне редко, а другие — чаще, чем должны были бы. Можно ли объяснить такой неудачный результат испытаний?

3.2.2. Другие методы

Конечно, линейные конгруэнтные последовательности — это не единственный источник случайных чисел, который предлагается для использования на компьютере. В этом разделе будет приведен обзор наиболее существенных альтернативных методов. Одни из них действительно важны, тогда как другие интересны главным образом потому, что они не так хороши, как хотелось бы.

В связи с получением случайных чисел возникает такая общепринятая ошибочная идея — достаточно взять хороший генератор случайных чисел и немного его модифицировать для того, чтобы получить "еще более случайную" последовательность. Часто это не так. Например, известно, что формула

$$X_{n+1} = (aX_n + c) \bmod m \tag{1}$$

позволяет получить более или менее хорошие случайные числа. Может ли последовательность, полученная из

$$X_{n+1} = \big((aX_n) \bmod (m+1) + c\big) \bmod m, \tag{2}$$

быть еще *более* случайной? Ответ: новая последовательность является *менее* случайной с большой долей вероятности. Таким образом, идея потерпела неудачу и при отсутствии какой-нибудь теории о поведении последовательности (2) мы попадаем в область генераторов типа $X_{n+1} = f(X_n)$ с выбранной наудачу функцией f. В упр. 3.1–11, 3.1–15 показано, что эти последовательности, вероятно, ведут себя намного хуже, чем последовательности, полученные при использовании более регулярных функций (1).

Давайте рассмотрим другой подход к попытке получить подлинно улучшенный вариант последовательности (1). Линейный конгруэнтный метод может быть обобщен, скажем, в квадратичный конгруэнтный метод:

$$X_{n+1} = (dX_n^2 + aX_n + c) \bmod m. \tag{3}$$

В упр. 8 обобщена теорема 3.2.1.2A, чтобы получить необходимые и достаточные условия для a, c и d, такие, чтобы последовательность, определенная соотношением (3), имела период максимальной длины m. В этом случае ограничения не более жесткие, чём в линейном методе.

Для m, которое является степенью 2, интересный квадратичный метод предложил Р. Р. Ковэю (R. R. Coveyou). Пусть

$$X_0 \bmod 4 = 2, \qquad X_{n+1} = X_n(X_n + 1) \bmod 2^e, \qquad n \geq 0. \tag{4}$$

Данная последовательность может быть вычислена приблизительно с той же эффективностью, что и (1), без любых беспокойств по поводу переполнения. Этот метод имеет интересную связь с подлинным методом средин квадратов фон Неймана (von Neumann). Если положить Y_n равным $2^e X_n$, так что Y_n является числом двойной точности, полученным в результате размещения справа e нулей у двоичного представления числа X_n, то Y_{n+1} точно совпадет со средними $2e$ цифрами $Y_n^2 + 2^e Y_n$! Другими словами, метод Ковэю в некоторой степени почти идентичен вырожденному методу средин квадратов двойной точности, однако он гарантирует получение длинного периода. Дополнительное свидетельство его случайности приведено в статье Ковэю, цитируемой в ответе к упр. 8.

Другие обобщения выражения (1) также очевидны. Например, можно попытаться увеличить длину периода последовательности. Период линейной конгруэнтной последовательности довольно длинный; когда m приблизительно равно длине слова компьютера, обычно получаются периоды порядка 10^9 или больше и в типичных вычислениях используется лишь маленькая часть последовательности. С другой стороны, при рассмотрении идеи "точности" в разделе 3.3.4 получается, что длина периода влияет на степень случайности последовательности. Значит, желательно получить длинный период и существует несколько подходящих для этого методов. Один из них состоит в том, чтобы сделать X_{n+1} зависящим от X_n и X_{n-1}, а не только от X_n. Тогда длина периода сможет достичь значения m^2, так как последовательность не станет повторяться, пока не будет получено равенство $(X_{n+\lambda}, X_{n+\lambda+1}) = (X_n, X_{n+1})$. Джон Мочли (John Mauchly) в неопубликованной работе, представленной на статистической конференции в 1949 году, расширил метод средин квадратов с помощью рекуррентного соотношения $X_n = \text{середина}\,(X_{n-1} \cdot X_{n-6})$.

Простейшая последовательность, в которой X_{n+1} зависит более чем от одного из предыдущих значений, — это последовательность чисел Фибоначчи

$$X_{n+1} = (X_n + X_{n-1}) \bmod m. \tag{5}$$

Данный генератор рассматривался в начале 50-х годов, и обычно он дает длину периода, бóльшую, чем m. Но тесты показывают, что числа, получаемые с помощью рекуррентного соотношения Фибоначчи, безусловно, *недостаточно* случайны, и, таким образом, выражение (5) нас, главным образом, интересует, как элегантный "плохой пример" источника случайных чисел. Можно также рассматривать генераторы вида

$$X_{n+1} = (X_n + X_{n-k}) \bmod m, \tag{6}$$

когда k — сравнительно большое число. Это рекуррентное соотношение было введено Грином, Смитом и Клем (Green, Smith, and Klem [*JACM* **6** (1959), 527–537]), сообщившими, что, когда $k \le 15$, тестирование последовательности с использованием критерия "интервалов", описанного в разделе 3.3.2, дала отрицательный результат, хотя при $k = 16$ результат был положительным.

Намного лучший аддитивный генератор был изобретен Дж. Ж. Митчелом (G. J. Mitchell) и Д. Ф. Муром (D. P. Moore) в 1958 году [не опубликовано]. Они предложили несколько необычную последовательность, определенную так:

$$X_n = (X_{n-24} + X_{n-55}) \bmod m, \qquad n \ge 55, \tag{7}$$

где m — четное число, а $X_0, \ldots, X_{54}$ — произвольные целые не все четные числа. Числа 24 и 55 в данном определении не были выбраны наудачу; эти специальные числа выбраны, оказывается, для того, чтобы определить такую последовательность, младшие значащие двоичные разряды $\langle X_n \bmod 2\rangle$ которой имеют длину периода $2^{55} - 1$. Очевидно, последовательность $\langle X_n\rangle$ должна иметь период по крайней мере такой же длины. В упр. 30 доказывается, что длина периода последовательности, определенной в выражении (7), точно равна $2^{e-1}(2^{55} - 1)$, когда $m = 2^e$.

На первый взгляд, рекуррентное соотношение (7) кажется не очень удобным для реализации на компьютере, но на самом деле существует эффективный путь генерирования этой последовательности с помощью циклической таблицы.

Алгоритм А (*Аддитивный генератор чисел*). В ячейки памяти $Y[1]$, $Y[2]$, ..., $Y[55]$ записано множество значений X_{54}, X_{53}, ..., X_0 соответственно; j вначале равно 24, а k равно 55. При реализации этого алгоритма на выходе последовательно получаем числа $X_{55}, X_{56}, \ldots$.

А1. [Суммирование.] (Если на выходе мы оказываемся в точке X_n, то $Y[j]$ равно X_{n-24}, а $Y[k]$ равно X_{n-55}.) Запишем $Y[k] \leftarrow (Y[k] + Y[j]) \bmod 2^e$, тогда на выходе получим $Y[k]$.

А2. [Продвижение.] Уменьшим j и k на 1. Если $j = 0$, то присвоим $j \leftarrow 55$; иначе, если $k = 0$, присвоить $k \leftarrow 55$. ▮

Этот алгоритм на компьютере MIX имеет следующий вид.

Программа А (*Аддитивный генератор чисел*). Если предположить, что индексные регистры 5 и 6, содержащие j и k, не затрагиваются частью программы, в которой эта подпрограмма размещена, то следующий текст программы реализует алгоритм А и заносит результат в регистр А.

```
LDA   Y,6   A1. Суммирование.
ADD   Y,5   Y_k + Y_j (возможно переполнение)
STA   Y,6       → Y_k.
DEC5  1     A2. Продвижение. j ← j − 1.
DEC6  1     k ← k − 1.
J5P   *+2
ENT5  55    Если j = 0, присвоить j ← 55.
J6P   *+2
ENT6  55    Если k = 0, присвоить k ← 55.   ▮
```

Этот генератор обычно работает быстрее других генераторов, обсуждавшихся ранее, так как он не требует никакого умножения. Кроме большой скорости выполнения этот алгоритм имеет самый длинный период из тех, которые встречались ранее, за исключением периода из упр. 3.2.1.2–22. Более того, как заметил Ричард Брент (Richard Brent), его можно реализовать в режиме работы с плавающей запятой, избегая преобразований целых чисел в дробные числа и наоборот (см. упр. 23). Поэтому можно доказать, что этот генератор является *наилучшим* источником случайных чисел для достижения практических целей. Основная причина, по которой трудно искренне рекомендовать последовательности, подобные (7), состоит в том, что получено очень мало теоретических результатов, основываясь на которых, можно проверить, имеет ли такая последовательность желаемые случайные свойства. Учитывая, как уже известно, что длинный период не всегда обеспечивает желаемые свойства, Джон Рейзер (John Reiser) (Ph. D. thesis, Stanford University, 1977) показал, однако, что аддитивные последовательности, подобные (7), будут в высокой степени хорошо распределены для больших размерностей, если обеспечить выполнение определенных приемлемых условий (см. упр. 26).

Числа 24 и 55 в (7) обычно называют *запаздыванием*, а числа X_n, определенные в (7), — *последовательностью Фибоначчи с запаздыванием*. Причины, по которым запаздывания, подобные (24, 55), работают хорошо, следуют из приведенных ниже теоретических результатов. Конечно, до некоторой степени легче использовать большие запаздывания, когда в приложениях случается применять, скажем, группы из 55 чисел одновременно. Среди чисел, генерируемых (7), никогда не найдется

Таблица 1

СМЕЩЕНИЯ, ПРИВОДЯЩИЕ К ДЛИННЫМ ПЕРИОДАМ ПО МОДУЛЮ 2

(24, 55)	(37, 100)	(83, 258)	(273, 607)	(576, 3217)	(7083, 19937)
(38, 89)	(30, 127)	(107, 378)	(1029, 2281)	(4187, 9689)	(9739, 23209)

Расширенные варианты этой таблицы приводятся в работах N. Zierler and J. Brillhart, *Information and Control* **13** (1968), 541–554, **14** (1969), 566–569, **15** (1969), 67–69; Y. Kurita and M. Matsumoto, *Math. Comp.* **56** (1991), 817–821; Heringa, Blöte, and Compagner, *Int. J. Mod. Phys.* **C3** (1992), 561–564.

значений X_n, лежащих строго между X_{n-24} и X_{n-55} (см. упр. 2). Ж.-М. Норманд (J.-M. Normand), Г. Й. Герман (H. J. Herrmann) и М. Хаджар (M. Hajjar) обнаружили небольшое смещение в числах, генерируемых (7), когда им понадобилось 10^{11} случайных чисел для проводимых с высокой точностью обширных исследований метода Монте-Карло [*J. Statistical Physics* **52** (1988), 441–446]; но при больших значениях k смещение уменьшалось. В табл. 1 приведено несколько пар чисел (l, k), для которых последовательность $X_n = (X_{n-l} + X_{n-k}) \bmod 2^e$ имеет период длиной $2^{e-1}(2^k - 1)$. Случая, когда $(l, k) = (30, 127)$, казалось бы, достаточно для большинства применений, особенно в сочетании с другими, увеличивающими случайность, методами, которые мы обсудим ниже.

Генератор случайных чисел во многом подобен сексу: когда он хорош — это прекрасно, когда он плох, все равно приятно (Джордж Марсалья, 1984).

Джордж Марсалья [*Comp. Sci. and Statistics: Symposium on the Interface* **16** (1984), 3–10] предложил заменить (7) на

$$X_n = (X_{n-24} \cdot X_{n-55}) \bmod m, \qquad n \geq 55, \tag{7'}$$

где m кратно 4, а все числа от X_0 до X_{54} нечетны, но сравнимы с 1 (по модулю 4). Тогда второстепенные младшие разряды имеют период $2^{55} - 1$, в то время как старшие двоичные разряды более тщательно перемешаны, чем раньше, так как они существенно зависят от всех разрядов X_{n-24} и X_{n-55}. В упр. 31 показано, что длина периода последовательности (7′) лишь незначительно меньше длины периода последовательности (7).

Генераторы последовательности Фибоначчи с запаздыванием успешно применялись во многих ситуациях с 1958 года. Таким образом, открытие в 90-е годы того, что они фактически провалились на крайне простом, незамысловатом критерии случайности, явилось шоком (см. упр. 3.3.2–31). Как избежать таких неприятностей, отбрасывая ненужные элементы последовательности, рассказывается в конце этого раздела.

Вместо рассмотрения исключительно аддитивных или исключительно мультипликативных последовательностей можно построить достаточно хороший генератор случайных чисел, используя всевозможные линейные комбинации $X_{n-1}, \ldots, X_{n-k}$ для малых k. В этом случае наилучший результат получается, когда модуль m является большим *простым числом*; например, m может быть выбрано так, чтобы оно было наибольшим простым числом, которое можно записать одним компьютерным словом (см. табл. 4.5.4–2). Когда $m = p$ — простое число, то по теории конечных полей можно найти множители $a_1, \ldots, a_k$, такие, что последовательность,

определенная соотношением

$$X_n = (a_1 X_{n-1} + \cdots + a_k X_{n-k}) \bmod p, \tag{8}$$

будет иметь период длиной $p^k - 1$. Здесь $X_0, \ldots, X_{k-1}$ могут быть выбраны произвольно, но так, чтобы все они не были нулями. (Частный случай, когда $k = 1$, соответствует мультипликативной конгруэнтной последовательности с уже известным простым модулем.) Константы $a_1, \ldots, a_k$ в (8) обладают подходящими свойствами тогда и только тогда, когда полином

$$f(x) = x^k - a_1 x^{k-1} - \cdots - a_k \tag{9}$$

является первообразным полиномом по модулю p, что выполняется тогда и только тогда, когда корень этого полинома есть первообразный элемент поля с p^k элементами (см. упр. 4.6.2–16).

Конечно, для достижения практических целей недостаточно простого факта *существования* подходящих констант a_1, ..., a_k, дающих период длиной $p^k - 1$. Необходимо быть в состоянии *найти* их, ведь нельзя проверить все p^k возможностей, так как p имеет порядок длины слова компьютера. К счастью, есть точно $\varphi(p^k - 1)/k$ подходящих наборов $(a_1, \ldots, a_k)$, поэтому в известной степени существует хороший шанс натолкнуться на один из них после нескольких случайных попыток. Но также следует уметь быстро определять, будет ли (9) первообразным полиномом по модулю p. Конечно, немыслимо генерировать до $p^k - 1$ элементов последовательности и ждать повторения! Методы проверки того, что полином будет первообразным по модулю p, обсуждались Аланеном (Alanen) и Кнутом (Knuth) в *Sankhyā* **A26** (1964), 305–328. Можно использовать следующий критерий. Пусть $r = (p^k - 1)/(p - 1)$.

i) $(-1)^{k-1} a_k$ должен быть первообразным корнем по модулю p (см. раздел 3.2.1.2).
ii) Полином x^r должен быть сравним с $(-1)^{k-1} a_k$ по модулям $f(x)$ и p.
iii) Степень $x^{r/q} \bmod f(x)$ (здесь используется арифметика полиномов по модулю p) должна быть положительной для каждого r — простого делителя q.

Эффективный способ вычисления полинома $x^n \bmod f(x)$ с использованием полиномиальной арифметики по модулю, заданному простым числом p, обсуждается в разделе 4.6.2.

Для того чтобы довести до конца тест, необходимо знать разложение на простые множители числа $r = (p^k - 1)/(p - 1)$, что и является ограничивающим фактором в вычислениях. r можно разложить на множители в приемлемый отрезок времени, когда $k = 2$, 3 и, возможно, 4, но большие значения k усложняют вычисления, когда p большое. Даже при $k = 2$ число "значащих случайных цифр", которое достигается при $k = 1$, по существу, удваивается, так что большие значения k вряд ли понадобятся.

Видоизмененный спектральный критерий (раздел 3.3.4) можно использовать для оценки последовательности чисел, генерируемых (8); см. упр. 3.3.4–24. Рассуждения, приведенные в этом разделе, показывают, что *не* следовало бы делать очевидный выбор ($a_1 = +1$ или -1), когда встречается такая форма первообразного полинома. Лучше выбрать большие, совершенно "случайные" значения $a_1, \ldots, a_k$, удовлетворяющие условиям, и проверить выбор с помощью спектрального критерия. Значительный объем вычислений приходится выполнять при возведении в

степень для нахождении $a_1, \ldots, a_k$. Но все известные доводы указывают на то, что результатом будет весьма удовлетворительный источник случайных чисел. Мы, по существу, добились случайности линейных конгруэнтных генераторов с k-кратной точностью, используя только операции с простой точностью.

Представляет интерес частный случай, когда $p = 2$. Иногда требуется генератор случайных чисел, вырабатывающий всего лишь случайную последовательность *двоичных разрядов* — нулей и единиц — вместо дробей, лежащих между нулем и единицей. Существует простой способ генерирования высокослучайных двоичных разрядов последовательности на бинарных компьютерах, основанный на манипулировании k-разрядными словами. Начать следует с произвольного ненулевого двоичного слова X. Затем необходимо вычислить следующий случайный бит последовательности, выполнив операции, которые приведены на языке компьютера MIX (см. упр. 16):

```
LDA  X      (Предположим, что переполнение сейчас "выключено".)
ADD  X      Перенести влево один разряд.
JNOV *+2    Перейти к другой команде, если исходное значение высшего
                разряда было нулем.                                    (10)
XOR  A      Иначе — установить число с "исключающим или".
STA  X
```

Четвертая операция "исключающее или" существует почти на всех двоичных компьютерах (см. упр. 2.5–28 и раздел 7.1). Она изменяет каждую позицию двоичного разряда rA, в ячейке A которой содержится "1". Содержимое ячейки A — это двоичная константа $(a_1 \ldots a_k)_2$, где $x^k - a_1 x^{k-1} - \cdots - a_k$ является первообразным полиномом по модулю 2, как упоминалось выше. После выполнения программы (10) следующим двоичным разрядом генерируемой последовательности можно взять младший двоичный разряд слова X. Или же можно последовательно выбирать старший двоичный разряд X, если он больше подходит.

Рассмотрим, например, рис. 1, на котором иллюстрируется генерируемая последовательность для $k = 4$ и СОДЕРЖИМОГО(A) $= (0011)_2$. Это, конечно, необычно малое значение k. В столбце показано, что последовательность двоичных разрядов последовательности, а именно — 1101011110001001..., повторяется с длиной периода $2^k - 1 = 15$. Эта последовательность совершенно случайна, если принять во внимание, что она была сгенерирована только с четырьмя двоичными разрядами памяти. Чтобы убедиться в этом, рассмотрим примыкающие множества четырех двоичных разрядов в периоде, а именно — 1101, 1010, 0101, 1011, 0111, 1111, 1110, 1100, 1000, 0001, 0010, 0100, 1001, 0011, 0110. Вообще говоря, каждое возможное примыкающее множество k двоичных разрядов однажды встречается в периоде, исключая множество всех нулей, так как длина периода равна $2^k - 1$. Таким образом, примыкающие множества k двоичных разрядов совершенно независимы. В разделе 3.5 показано, что это очень сильный критерий случайности, когда k равняется, скажем, 30 или больше. Теоретические результаты, иллюстрирующие случайность этой последовательности, приведены в статье Р. К. Таусворта (R. C. Tausworthe, *Math. Comp.* **19** (1965), 201–209).

1011
0101
1010
0111
1110
1111
1101
1001
0001
0010
0100
1000
0011
0110
1100
1011

Рис. 1. Последовательные значения компьютерного слова X в бинарном методе, если предположить, что $k = 4$ и СОДЕРЖИМОЕ(A) $= (0011)_2$.

Первообразный полином по модулю 2 степени ≤ 168 табулирован В. Станке (W. Stahnke, *Math. Comp.* **27** (1973), 977–980.) Когда $k = 35$, можем взять

$$\text{СОДЕРЖИМОЕ(A)} = (00000000000000000000000000000000101)_2,$$

но, принимая во внимание упр. 18 и 3.3.4–24, приходим к заключению, что лучше найти "случайные" константы, определяющие первообразный полином по модулю 2.

Предостережение. Кое-кто обманывается, полагая, что техника случайного поразрядного генерирования может использоваться для генерирования случайных дробей, которые занимают целое слово $(X_0X_1\ldots X_{k-1})_2$, $(X_kX_{k+1}\ldots X_{2k-1})_2$, ... Но на самом деле это скудный источник случайных дробей, даже несмотря на то, что отдельный двоичный разряд совершенно случаен. В упр. 18 объясняется, почему так происходит.

Аддитивный генератор (7) Митчела (Mitchell) и Мура (Moore) в основном базируется на концепции первообразных полиномов: полином $x^{55} + x^{24} + 1$ является первообразным, а табл. 1 — это, по существу, таблица определенных первообразных трехчленов по модулю 2. Почти идентичный генератор независимо от Митчела и Мура открыли в 1971 году Т. Ж. Левис (T. G. Lewis) и В. Г. Пэйн (W. H. Payne) [*JACM* **20** (1973), 456–468], но они использовали операцию "исключающее или" вместо суммирования. Это делает длину периода равной точно $2^{55} - 1$. Каждая позиция двоичного разряда в последовательности Левиса и Пэйна пробегает ту же периодическую последовательность, но имеет собственную начальную позицию. Опыт показал, что (7) дает лучшие результаты.

Мы сейчас увидим, что последовательности с $0 \le X_n < m$ и периодом $m^k - 1$ могут быть построены без больших усилий, где X_n — подходящая функция от $X_{n-1}, \ldots, X_{n-k}$ и m — простое число. Наибольший возможный период для *любой* последовательности, определенной соотношением вида

$$X_n = f(X_{n-1}, \ldots, X_{n-k}), \qquad 0 \le X_n < m, \tag{11}$$

как легко видеть, равен m^k. М. Г. Мартин (M. H. Martin) [*Bull. Amer. Math. Soc.* **40** (1934), 859–864] первым показал, что для всех m и k существуют функции, позволяющие достичь максимального периода. Его метод можно легко сформулировать (упр. 17) и достаточно эффективно запрограммировать (см. упр. 29), но он непригоден для генерирования случайных чисел, потому что изменение значений $X_{n-1} + \cdots + X_{n-k}$ — очень медленный процесс: все строки размерностью k встречаются, но в не совсем случайном порядке. Лучший класс функций f,

дающих максимальный период m^k, рассмотрен в упр. 21. Подобные программы, вообще говоря, не так эффективны для генератора случайных чисел, как другие уже описанные методы, но, когда речь идет о периоде в целом, они все-таки производят достаточно случайные последовательности.

Для генерирования случайных чисел предложено множество других схем. Наиболее интересным из этих альтернативных методов является, возможно, *обратная конгруэнтная последовательность*, предложенная Эйченауэром (Eichenauer) и Лехном (Lehn) [*Statistische Hefte* **27** (1986), 315–326]:

$$X_{n+1} = (aX_n^{-1} + c) \bmod p. \tag{12}$$

Здесь p — простое число, X_n принимает значения из множества $\{0, 1, \ldots, p-1, \infty\}$, а обращение определено как $0^{-1} = \infty$, $\infty^{-1} = 0$. В других случаях $X^{-1}X \equiv 1$ (по модулю p). Так как 0 всегда следует за ∞, а затем за c в этой последовательности, можно было бы просто определить $0^{-1} = 0$ для удобства реализации, но теория является цельной и естественной, когда $0^{-1} = \infty$. Существуют эффективные алгоритмы, которые можно реализовать на вычислительных машинах, пригодные для вычислений X^{-1} (по модулю p) (см., например, упр. 4.5.2–39). К несчастью, однако, операций, используемых в этих алгоритмах, в большинстве компьютеров нет. В упр. 35 показано, как много выборов a и c приводят к максимальному периоду длиной $p + 1$. В упр. 37 продемонстрированы наиболее важные свойства: обратная конгруэнтная последовательность совершенно лишена решетчатой структуры, что характерно для линейных конгруэнтных последовательностей.

Другой важный класс методов связан с *комбинацией* генераторов случайных чисел.

Всегда найдутся сторонники того, что линейные конгруэнтные, аддитивные и другие методы слишком просты для того, чтобы давать достаточно случайную последовательность, и невозможно будет *доказать*, что такой скептицизм необоснован. Может быть, они в самом деле правы, так что совершенно бесполезно обсуждать этот вопрос. Существует достаточно эффективный способ объединения двух последовательностей в третью, которая была бы настолько случайной, что удовлетворяла бы всех, кроме совершенно убежденных скептиков.

Допустим, имеются последовательности $X_0, X_1, \ldots$ и $Y_0, Y_1, \ldots$ случайных чисел, лежащих между 0 и $m - 1$ и предпочтительно сгенерированных двумя различными методами. Тогда можно, например, использовать одну случайную последовательность для изменения порядка элементов другой, как предложили М. Д. Мак-Ларен (M. D. MacLaren) и Дж. Марсалья (G. Marsaglia) [*JACM* **12** (1965), 83–89; см. также работу Марсалья и Брея (Bray), *CACM* **11** (1968), 757–759].

Алгоритм M (*Рандомизация перемешиванием*). Если заданы методы генерирования двух последовательностей $\langle X_n \rangle$ и $\langle Y_n \rangle$, этот алгоритм будет последовательно генерировать элементы "значительно более случайной" последовательности. Воспользуемся вспомогательной таблицей $V[0], V[1], \ldots, V[k-1]$, где k — некоторое число, для удобства обычно выбираемое приблизительно равным 100. Вначале V-таблица заполняется первыми k значениями X-последовательности.

M1. [Генерирование X, Y.] Положим X и Y равными следующим членам последовательностей $\langle X_n \rangle$ и $\langle Y_n \rangle$ соответственно.

M2. [Выбор j.] Присвоим $j \leftarrow \lfloor kY/m \rfloor$, где m — модуль, используемый в последовательности $\langle Y_n \rangle$, т. е. j — случайная величина, определяемая Y, $0 \le j < k$.

M3. [Замена.] Выведем $V[j]$, а затем присвоим $V[j] \leftarrow X$. ▮

Предположим, например, что алгоритм M применяется к таким двум последовательностям при $k = 64$:

$$\begin{aligned} X_0 &= 5772156649, \qquad X_{n+1} = (3141592653X_n + 2718281829) \bmod 2^{35}; \\ Y_0 &= 1781072418, \qquad Y_{n+1} = (2718281829Y_n + 3141592653) \bmod 2^{35}. \end{aligned} \tag{13}$$

Интуиция подсказывает, что последовательность, полученная в результате реализации алгоритма M (13), удовлетворяет *любым* требованиям случайности, которые предъявляются к генерируемым на компьютере последовательностям, поскольку зависимость между соседними выходными элементами почти полностью исключена. Более того, время генерирования этой последовательности лишь незначительно превышает удвоенное время, необходимое для генерирования последовательности $\langle X_n \rangle$.

В упр. 15 показано, что в ситуациях, представляющих наибольший практический интерес, длина периода последовательности, которая получается при реализации алгоритма M, равна наименьшему общему кратному длин периодов $\langle X_n \rangle$ и $\langle Y_n \rangle$. В частности, если отбросить значение 0, когда оно встречается в Y-последовательности, так что $\langle Y_n \rangle$ имеет период длиной $2^{35} - 1$, то числа, генерируемые алгоритмом M из рекуррентных соотношений (13), будут иметь период длиной $2^{70} - 2^{35}$. (См. работу Дж. Артура Гринвуда [J. Arthur Greenwood, *Comp. Sci. and Statistics: Symp. on the Interface* **9** (1976), 222].)

Однако существует еще лучший путь перемешивания элементов последовательности, открытый Картером Бейсом (Carter Bays) и С. Д. Дархамом (S. D. Durham) [*ACM Trans. Math. Software* **2** (1976), 59–64]. Хотя их подход и появился для того, чтобы несколько упростить алгоритм M, неожиданно оказалось, что он может дать лучшие результаты, чем алгоритм M, даже несмотря на то, что на входе он требует только одну последовательность $\langle X_n \rangle$ вместо двух.

Алгоритм B (*Рандомизация перемешиванием*). Если задан метод генерирования последовательности $\langle X_n \rangle$, этот алгоритм будет последовательно выводить элементы "значительно более случайной" последовательности, используя вспомогательную таблицу $V[0], V[1], \ldots, V[k-1]$, как и в алгоритме M. Вначале V-таблица заполняется первыми k значениями X-последовательности, а вспомогательную переменную Y положим равной $k+1$-му значению.

B1. [Выбор j.] Присвоим $j \leftarrow \lfloor kY/m \rfloor$, где m — модуль, используемый в последовательности $\langle X_n \rangle$; т. е. j — это случайная величина, определяемая Y, $0 \le j < k$.

B2. [Замена.] Выведем $V[j]$, присвоим $V[j] \leftarrow X$, выведем $V[j]$ и установим $V[j]$ следующим членом последовательности $\langle X_n \rangle$. ▮

Желание почувствовать различие между алгоритмами M и B побудит читателя заняться упр. 3 и 5.

На компьютере MIX можно реализовать алгоритм B, взяв k равным размеру байта и выполнив вычисления в соответствии со следующей простой программой

генерирования случайных чисел.

```
LD6  Y(1:1)   j ← старший разряд байта Y.
LDA  X        rA ← X_n.
INCA 1        (См. упр. 3.2.1.1–1.)
MUL  A        rX ← X_{n+1}.
STX  X        "n ← n + 1."
LDA  V,6                                   (14)
STA  Y        Y ← V[j].
STX  V,6      V[j] ← X_n.  ▮
```

Выход появляется в регистре A. Заметим, что алгоритм B требует всего четыре дополнительные операции для генерирования числа.

Ф. Гебхардт (F. Gebhardt) [*Math. Comp.* **21** (1967), 708–709] нашел, что удовлетворительная случайная последовательность порождается алгоритмом M, даже когда он применяется к такой неслучайной последовательности, как последовательность Фибоначчи, с $X_n = F_{2n} \bmod m$ и $Y_n = F_{2n+1} \bmod m$. Однако для алгоритма M также возможно получение последовательности, *менее* случайной, чем исходная последовательность, если $\langle X_n \rangle$ и $\langle Y_n \rangle$ строго зависимы, как в упр. 3. Такие проблемы, кажется, не возникают с алгоритмом B. Поскольку алгоритм B не делает никакую последовательность менее случайной и очень мала цена увеличения случайности, он может быть рекомендован к использованию с любым другим генератором случайных чисел.

Однако методы перемешивания имеют "врожденный дефект" Они изменяют порядок следования генерируемых чисел, но не сами числа. В большинстве случаев порядок следования является решающим фактором, но, если генератор случайных чисел не удовлетворяет "критерию промежутков между днями рождений", обсуждаемому в разделе 3.3.2, или критерию случайных блужданий из упр. 3.3.2–31, то положение после перемешивания не улучшится. Перемешивание имеет еще одно сравнительное неудобство, заключающееся в том, что оно не позволяет стартовать с заданного места в периоде либо быстро перемещаться из X_n в X_{n+k} при больших k.

Многие поэтому советуют объединять последовательности $\langle X_n \rangle$ и $\langle Y_n \rangle$ более простым способом, лишенным дефектов перемешивания. Например, можно использовать объединение вида

$$Z_n = (X_n - Y_n) \bmod m, \tag{15}$$

где $0 \le X_n < m$ и $0 \le Y_n < m' \le m$. В упр. 13 и 14 обсуждается длина периода таких последовательностей; в упр. 3.3.2–23 показано, что (15) имеет тенденцию к увеличению случайности, если начальные значения X_0 и Y_0 выбираются независимо.

Простой метод устранения структурных смещений арифметически генерируемых чисел был предложен на заре программирования Дж. Тоддом (J. Todd) и О. Таусски Тодд (O. Taussky Todd) [*Symp. on Monte Carlo Methods* (Wiley, 1956), 15–28]. Мы можем просто выбросить несколько чисел последовательности. Их предложение мало использовалось в линейных конгруэнтных генераторах, но оно стало использоваться сейчас в связи с появлением генераторов, подобных (7), имеющих очень длинный период, потому что есть сколько угодно чисел, которые можно отбросить.

Простейшим путем улучшения случайности (7) является использование только каждого j-го элемента для некоторого малого j. Но лучшим способом, возможно,

еще более простым, является применение (7) для получения, скажем, массива из 500 случайных чисел и использование только первых 55 чисел. После этого таким же методом генерируются следующие 500 чисел. Эта идея была предложена Мартином Люшером (Martin Lüscher) [*Computer Physics Communications* **79** (1994), 100–110]. Толчком послужила теория хаоса в динамических системах. Можно рассматривать (7) как процесс преобразования 55 значений $(X_{n-55}, \ldots, X_{n-1})$ в другой вектор из 55 значений $(X_{n+t-55}, \ldots, X_{n+t-1})$. Предположим, что генерируется $t \geq 55$ значений, а используются первые 55. Тогда, если $t = 55$, новый вектор значений в некоторой степени близок старому; но, если $t \approx 500$, старый и новый векторы всегда не коррелируют между собой (см. упр. 33). Для аналогичного случая генераторов суммирования с переносом или вычитания с заимствованием (упр. 3.2.1.1–14), как известно, векторы будут представлениями чисел в b-ичной системе счисления в линейном конгруэнтном генераторе, а подходящим множителем, когда генерируется сразу t чисел, будет b^{-t}. Теория Люшера в этом случае, следовательно, может быть подтверждена спектральным критерием из раздела 3.3.4. Портативный генератор случайных чисел, основанный на последовательности Фибоначчи с запаздыванием, усиленный методом Люшера, рассматривается в разделе 3.6, в котором приведены и комментарии.

Генераторы случайных чисел, как правило, выполняют лишь незначительное число умножений и/или суммирований при переходе от одного члена последовательности к другому. Когда такие генераторы комбинируются, как рассказывалось выше, здравый смысл говорит нам, что полученная последовательность не должна отличаться от настоящей случайной последовательности. Однако интуиция не может заменить строгое математическое доказательство. Если поработать дольше (скажем, 1 000 или 1 000 000 часов), можно получить последовательности, для которых, по существу, имеются лучшие теоретические гарантии случайности.

Например, рассмотрим последовательность двоичных разрядов $B_1, B_2, \ldots$, генерируемую соотношением

$$X_{n+1} = X_n^2 \bmod M, \qquad B_n = X_n \bmod 2 \tag{16}$$

(см. работу Blum, Blum, and Shub, *SICOMP* **15** (1986), 364–383), или более сложную последовательность, генерируемую соотношением

$$X_{n+1} = X_n^2 \bmod M, \qquad B_n = X_n \cdot Z \bmod 2, \tag{17}$$

где скалярное произведение r-разрядных двоичных чисел $(x_{r-1} \ldots x_0)_2$ и $(z_{r-1} \ldots z_0)_2$ равно $x_{r-1}z_{r-1} + \cdots + x_0 z_0$. Здесь Z — r-разрядная "маска", а r — число двоичных разрядов в M. Модуль M может быть произведением двух больших простых чисел вида $4k+3$, а начальное значение X_0 — взаимно простым числом с M. Правило (17), предложенное Леонидом Левиным, является обобщением метода средин квадратов фон Неймана; мы будем называть его *смешанно-квадратичным методом*, потому что он перемешивает квадраты двоичных разрядов. Правило (16), конечно, является частным случаем для $Z = 1$. В разделе 3.5F содержится доказательство того, что, когда X_0, Z и M выбраны наудачу, последовательность, сгенерированная соотношениями (16) и (17), удовлетворяет всем статистическим критериям случайности; на генерирование такой последовательности требуется усилий не больше, чем на умножение больших чисел. Другими словами, двоичные разряды неотличимы от

действительно случайных чисел для любых вычислений, длящихся менее ста лет, на современных быстродействующих компьютерах, когда M достаточно велико. Если это не так, то можно найти множители нетривиальных частей таких чисел намного быстрее, чем известно сейчас. Формула (16) проще, чем (17), но модуль M в (16) должен быть несколько больше, чем в (17), если необходимо получить те же статистические гарантии.

УПРАЖНЕНИЯ

▶ **1.** [*12*] На практике случайные числа формируются с помощью $X_{n+1} = (aX_n + c) \bmod m$, где X_n — *целые числа*, которые впоследствии рассматриваются как *дроби* $U_n = X_n/m$. Рекуррентное соотношение для U_n на самом деле имеет вид

$$U_{n+1} = (aU_n + c/m) \bmod 1.$$

Объясните, как генерируется случайная последовательность с помощью этого соотношения, *непосредственно* используя арифметику с плавающей точкой компьютера.

▶ **2.** [*M20*] В хорошем источнике случайных чисел неравенства $X_{n-1} < X_{n+1} < X_n$ будут встречаться примерно один раз из шести, так как каждое из шести возможных отношений порядка X_{n-1}, X_n и X_{n+1} должно иметь одну и ту же вероятность. Покажите, однако, что приведенный выше порядок *никогда* не возникнет, если использовать последовательность Фибоначчи (5).

3. [*23*] (a) Какую последовательность генерирует алгоритм M, если

$$X_0 = 0, \quad X_{n+1} = (5X_n + 3) \bmod 8, \qquad Y_0 = 0, \quad Y_{n+1} = (5Y_n + 1) \bmod 8$$

и $k = 4$? (Заметим, что потенциал равен двум, т. е. $\langle X_n \rangle$ и $\langle Y_n \rangle$ не настолько случайны, чтобы стоило их использовать.) (b) Что случится, если алгоритм B применить к этой же последовательности $\langle X_n \rangle$ с $k = 4$?

4. [*00*] Почему наибольший значащий байт используется в первой строке программы (14) вместо других?

▶ **5.** [*20*] Обсудите, стоит ли использовать $X_n = Y_n$ в алгоритме M для того, чтобы повысить скорость генерирования. Будет ли результат аналогичен результату, полученному с использованием алгоритма B?

6. [*10*] В бинарном методе (10) младший разряд `X` случаен, если программа многократно повторяется. Почему все *слово* `X` не случайно?

7. [*20*] Покажите, что можно получить полную последовательность длиной 2^e (т. е. последовательность, в которой каждое из 2^e возможных множеств e примыкающих разрядов встречается только один раз за период), если программу (10) изменить следующим образом.

```
LDA  X          LDA  A          JNOV *+3        XOR  A
JANZ *+2        ADD  X          JAZ  *+2        STA  X
```

8. [*M39*] Докажите, что квадратичная конгруэнтная последовательность (3) имеет период длиной m тогда и только тогда, когда выполняются следующие условия:

i) *c и m — взаимно простые числа;*
ii) *d и $a - 1$ кратны p для всех p — нечетных простых делителей m;*
iii) *d четно и $d \equiv a - 1$* (по модулю 4), *если m кратно* 4;
$d \equiv a - 1$ (по модулю 2), *если m кратно* 2;
iv) $d \not\equiv 3c$ (по модулю 9), *если m кратно* 9.

[*Указание.* Последовательность, определенная как $X_0 = 0$, $X_{n+1} = dX_n^2 + aX_n + c$, по модулю m имеет период длиной m тогда и только тогда, когда эта же последовательность по модулю r имеет период длиной r, где r — делитель m.]

▸ **9.** [*M24*] (P. R. Ковэю (R. R. Coveyou).) Используйте результаты упр. 8 для доказательства того, что длина периода модифицированного метода средин квадратов (4) равна 2^{e-2}.

10. [*M29*] Покажите, что если X_0 и X_1 — такие простые числа, что по крайней мере одно из них нечетно, и $m = 2^e$, то период последовательности Фибоначчи (5) равен $3 \cdot 2^{e-1}$.

11. [*M36*] Назначение этого упражнения состоит в анализе определенных свойств последовательности целых чисел, удовлетворяющих рекуррентному соотношению

$$X_n = a_1 X_{n-1} + \cdots + a_k X_{n-k}, \qquad n \geq k.$$

Если можно вычислить длину периода данной последовательности по модулю $m = p^e$, когда p — простое число, то длина периода этой последовательности по отношению к произвольному модулю m равна наименьшему общему кратному длин периодов последовательностей, для которых модуль равен степеням простых сомножителей m.

a) Если $f(z)$, $a(z)$, $b(z)$ — это полиномы с целыми коэффициентами, то запишем $a(z) \equiv b(z)$ по модулям $f(z)$ и m, если $a(z) = b(z) + f(z)u(z) + mv(z)$ для некоторых полиномов $u(z)$ и $v(z)$ с целыми коэффициентами. Докажите, что имеет место следующее утверждение, когда $f(0) = 1$ и $p^e > 2$: если $z^\lambda \equiv 1$ по модулям $f(z)$ и p^e и $z^\lambda \not\equiv 1$ по модулям $f(z)$ и p^{e+1}, то $z^{p\lambda} \equiv 1$ по модулям $f(z)$ и p^{e+1} и $z^{p\lambda} \not\equiv 1$ по модулям $f(z)$ и p^{e+2}.

b) Пусть $f(z) = 1 - a_1 z - \cdots - a_k z^k$ и

$$G(z) = 1/f(z) = A_0 + A_1 z + A_2 z^2 + \cdots.$$

Пусть $\lambda(m)$ обозначает длину периода $\langle A_n \bmod m \rangle$. Докажите, что $\lambda(m)$ — наименьшее положительное λ, такое, что $z^\lambda \equiv 1$ по модулям $f(z)$ и m.

c) Дано: p — простое число, $p^e > 2$ и $\lambda(p^e) \neq \lambda(p^{e+1})$. Докажите, что $\lambda(p^{e+r}) = p^r \lambda(p^e)$ для всех $r \geq 0$. (Таким образом, чтобы найти длину периода последовательности $\langle A_n \bmod 2^e \rangle$, можно подсчитывать $\lambda(4)$, $\lambda(8)$, $\lambda(16)$, ..., пока не будет найдено наименьшее $e \geq 3$, такое, что $\lambda(2^e) \neq \lambda(4)$. Тогда длина периода будет определена по $\bmod 2^e$ для всех e. В упр. 4.6.3–26 объясняется, как вычислить X_n для больших n за $O(\log n)$ операций.)

d) Покажите, что любая последовательность целых чисел, которая удовлетворяет рекуррентному соотношению, сформулированному в начале этого упражнения, имеет производящую функцию $g(z)/f(z)$ для некоторого полинома $g(z)$ с целыми коэффициентами.

e) Дано, что полиномы $f(z)$ и $g(z)$ в п. (d) взаимно просты по модулю p (см. раздел 4.6.1). Докажите, что последовательность $\langle X_n \bmod p^e \rangle$ имеет ту же длину периода, что и специальная последовательность $\langle A_n \bmod p^e \rangle$ в (b). (Нельзя увеличить длину периода путем выбора *любых* $X_0, \ldots, X_{k-1}$, так как общая последовательность является линейной комбинацией "сдвигов" специальной последовательности.) [*Указание.* Из упр. 4.6.2–22 (лемма Хенселя) следует, что существуют полиномы, такие, что $a(z)f(z) + b(z)g(z) \equiv 1$ (по модулю p^e).]

▸ **12.** [*M28*] Найдите целые числа X_0, X_1, a, b и c, такие, что последовательность

$$X_{n+1} = (aX_n + bX_{n-1} + c) \bmod 2^e, \qquad n \geq 1,$$

имеет самый длинный период среди всех последовательностей этого типа. [*Указание.* Можно показать, что $X_{n+2} = ((a+1)X_{n+1} + (b-a)X_n - bX_{n-1}) \bmod 2^e$; см. упр. 11, (c).]

13. [*M20*] Пусть $\langle X_n \rangle$ и $\langle Y_n \rangle$ — последовательности целых чисел по $\bmod m$ с периодами длиной λ_1 и λ_2. Объединим их, положив $Z_n = (X_n + Y_n) \bmod m$. Покажите, что если λ_1 и λ_2 — взаимно простые числа, то последовательность $\langle Z_n \rangle$ имеет период длиной $\lambda_1 \lambda_2$.

14. [*M24*] Пусть X_n, Y_n, Z_n, λ_1 и λ_2 определены так же, как в предыдущем упражнении. Предположим, что разложение λ_1 на простые множители имеет вид $2^{e_2}3^{e_3}5^{e_5}\ldots$ и аналогично $\lambda_2 = 2^{f_2}3^{f_3}5^{f_5}\ldots$. Пусть $g_p = (\max(e_p, f_p)$, если $e_p \neq f_p$, в других случаях — 0) и пусть $\lambda_0 = 2^{g_2}3^{g_3}5^{g_5}\ldots$. Покажите, что длина периода λ' последовательности $\langle Z_n\rangle$ кратна λ_0 и является делителем $\lambda = \operatorname{lcm}(\lambda_1, \lambda_2)$. В частности, $\lambda' = \lambda$, если ($e_p \neq f_p$ или $e_p = f_p = 0$) для каждого простого p.

15. [*M27*] Пусть последовательность $\langle X_n\rangle$ в алгоритме M имеет длину периода λ_1 и все элементы в этом периоде различны. Пусть $q_n = \min\{r \mid r > 0$ и $\lfloor kY_{n-r}/m\rfloor = \lfloor kY_n/m\rfloor\}$. Предположим, что $q_n < \frac{1}{2}\lambda_1$ для всех $n \geq n_0$ и что последовательность $\langle q_n\rangle$ имеет длину периода λ_2. Пусть λ — наименьшее общее кратное λ_1 и λ_2. Докажите, что последовательность на выходе $\langle Z_n\rangle$, полученная с помощью алгоритма M, имеет длину периода λ.

▶ **16.** [*M28*] Пусть в методе (10) СОДЕРЖИМОЕ(A) равно $(a_1a_2\ldots a_k)_2$ в бинарной записи. Покажите, что последовательность, генерируемая младшими разрядами X_0, X_1, ..., удовлетворяет соотношению

$$X_n = (a_1X_{n-1} + a_2X_{n-2} + \cdots + a_kX_{n-k}) \bmod 2.$$

[Это можно рассматривать как другой способ определения последовательности, хотя связь между данным соотношением и программой (10), на первый взгляд, не заметна!]

17. [*M33*] (М. Х. Мартин (M. H. Martin), 1934.) Пусть m и k — положительные числа и пусть $X_1 = X_2 = \cdots = X_k = 0$. Для всех $n > 0$ положим X_{n+k} равным наибольшему неотрицательному числу $y < m$, такому, что k-мерная строка $(X_{n+1}, \ldots, X_{n+k-1}, y)$ еще не появилась в последовательности. Другими словами, $(X_{n+1}, \ldots, X_{n+k-1}, y)$ должна отличаться от $(X_{r+1}, \ldots, X_{r+k})$ для $0 \leq r < n$. При этом каждая возможная k-мерная строка встретится по крайней мере один раз в последовательности. В конце концов процесс закончится, когда будет достигнуто такое значение n, при котором строка $(X_{n+1}, \ldots, X_{n+k-1}, y)$ уже появлялась в последовательности для всех неотрицательных $y < m$. Например, если $m = k = 3$, такой последовательностью будет 000222122021121020120011101 00 и процесс закончится в этой точке. (a) Докажите, что, когда последовательность закончится, будут выполняться равенства $X_{n+1} = \cdots = X_{n+k-1} = 0$. (b) Докажите, что *каждая* k-мерная строка элементов $(a_1, a_2, \ldots, a_k)$, таких, что $0 \leq a_j < m$, появляется в последовательности. Поэтому последовательность окончится при $n = m^k$. [*Указание.* Докажите, что k-мерная строка $(a_1, \ldots, a_s, 0, \ldots, 0)$ появляется, когда $a_s \neq 0$, используя индукцию по s.] Заметим, что если сейчас определить $f(X_n, \ldots, X_{n+k-1}) = X_{n+k}$ для $1 \leq n \leq m^k$, полагая $X_{m^k+k} = 0$, то получится функция с максимальным возможным периодом.

18. [*M22*] Пусть $\langle X_n\rangle$ — это последовательность двоичных разрядов, генерируемая методом (10), с $k = 35$ и СОДЕРЖИМОЕ(A) $= (00000000000000000000000000000101)_2$.

Пусть U_n — бинарная дробь $(.X_{nk}X_{nk+1}\ldots X_{nk+k-1})_2$. Покажите, что эта последовательность $\langle U_n\rangle$ не удовлетворяет сериальному критерию пар (раздел 3.3.2B), когда $d = 8$.

19. [*M41*] Для каждого простого числа p из первого столбца табл. 2 раздела 4.5.4 найдите подходящие константы a_1 и a_2, как предлагается в разделе, чтобы длина периода (8) при $k = 2$ равнялась $p^2 - 1$. (Например, см. рекуррентное соотношение 3.3.4–(39).)

20. [*M40*] Вычислите подходящие константы для использования в качестве содержимого регистра A (СОДЕРЖИМОЕ(A)) в методе (10), имеющие приблизительно то же количество нулей, что и константы для $2 \leq k \leq 64$.

21. [*M35*] (Д. Рис (D. Rees).) В разделе объясняется, как найти функции f, такие, что последовательность (11) имеет длину периода $m^k - 1$, если m — простое число и не все $X_0, \ldots, X_{k-1}$ равны нулю. Покажите, что такие функции могут быть изменены для получения последовательности наподобие (11) с длиной периода m^k для *всех* целых m.

[*Указание.* Рассмотрите лемму 3.2.1.2Q, трюк из упр. 7 и последовательность вида $\langle pX_{2n} + X_{2n+1}\rangle$.]

▸ **22.** [*M24*] В разделе нет обширных обсуждений способов расширения линейной последовательности (8) до случая, когда m является простым числом. Докажите, что достаточно длинный период может быть получен, когда m "свободно от квадратов", т. е. является произведением различных простых чисел. (Из табл. 3.2.1.1–1 ясно, что $m = w \pm 1$ часто удовлетворяет этим предположениям. Многие из результатов, приведенных в настоящем разделе, могут поэтому быть распространены на случай, который в некоторой степени более удобен для вычислений.)

▸ **23.** [*20*] Рассмотрите последовательность $X_n = (X_{n-55} - X_{n-24}) \bmod m$ как альтернативу последовательности (7).

24. [*M20*] Пусть $0 < l < k$. Докажите, что последовательность двоичных разрядов, определенная рекуррентным соотношением $X_n = (X_{n-k+l} + X_{n-k}) \bmod 2$, имеет длину периода $2^k - 1$ всякий раз, когда такой же период имеет последовательность, определенная соотношением $Y_n = (Y_{n-l} + Y_{n-k}) \bmod 2$.

25. [*26*] Рассмотрите альтернативу для программы A, состоящую в том, что все 55 входов в таблице Y-в заменяются 55 раз требуемыми случайными числами.

26. [*M48*] (Дж. Ф. Рейзер (J. F. Reiser).) Пусть p — простое число и k — положительное число. Пусть заданы целые числа $a_1, \ldots, a_k$ и $x_1, \ldots, x_k$, пусть λ_α — период последовательности $\langle X_n\rangle$, заданной рекуррентным соотношением

$$X_n = x_n \bmod p^\alpha, \quad 0 \le n < k; \qquad X_n = (a_1 X_{n-1} + \cdots + a_k X_{n-k}) \bmod p^\alpha, \quad n \ge k,$$

и пусть N_α равно числу нулей, которые встречаются в периоде (числу индексов j, таких, что $\mu_\alpha \le j < \mu_\alpha + \lambda_\alpha$ и $X_j = 0$). Докажите или опровергните следующее утверждение: существует константа c (зависящая, возможно, от p, k и $a_1, \ldots, a_k$), такая, что $N_\alpha \le cp^{\alpha(k-2)/(k-1)}$ для всех α и всех $x_1, \ldots, x_k$.

[*Замечание.* Рейзер доказал, что если рекуррентная последовательность имеет максимальную длину периода по модулю p (т. е. если $\lambda_1 = p^k - 1$) и если утверждение имеет место, то k-мерное расхождение $\langle X_n\rangle$ будет равно $O(\alpha^k p^{-\alpha/(k-1)})$ при $\alpha \to \infty$. Таким образом, аддитивный генератор, подобный (7), был бы распределен в 55 измерениях, когда $m = 2^e$ и рассматривается полный период. (См. раздел 3.3.4, в котором определено понятие расхождения в k измерениях.) Утверждение является слабым условием, если $\langle X_n\rangle$ принимает каждое значение примерно одинаково часто и если $\lambda_\alpha = p^{\alpha-1}(p^k - 1)$. Величина $N_\alpha \approx (p^k - 1)/p$ не увеличивается, вообще говоря, когда α возрастает. Рейзер проверил это утверждение для $k = 3$. С другой стороны, он показал, что можно найти необычайно плохие (зависящие от α) начальные значения $x_1, \ldots, x_k$, такие, что $N_{2\alpha} \ge p^\alpha$, обеспечивающие $\lambda_\alpha = p^{\alpha-1}(p^k - 1)$, $k \ge 3$, α достаточно большое.]

27. [*M30*] Предположим, что алгоритм B применяется к последовательности $\langle X_n\rangle$ с длиной периода λ, где $\lambda \gg k$. Покажите, что для фиксированного k и всех достаточно больших λ последовательность на выходе будет периодичной с той же самой длиной периода λ, если $\langle X_n\rangle$ не является слишком случайной. [*Указание.* Найдите структуру последовательных значений $\lfloor kX_n/m\rfloor$, которая обеспечивает "синхронизацию" дальнейшего поведения алгоритма B.]

28. [*40*] (А. Дж. Вотерман (A. G. Waterman).) Исследуйте линейную конгруэнтную последовательность с m, равным квадрату или кубу длины компьютерного слова, в то время как a и c заданы с обычной точностью.

▸ **29.** [*40*] Найдите хороший метод вычисления функции $f(x_1, \ldots, x_k)$, определенной последовательностью Мартина (Martin) в упр. 17, если задана только строка $(x_1, \ldots, x_k)$ размерности k.

30. [*M37*] (P. П. Брент (R. P. Brent).) Пусть $f(x) = x^k - a_1x^{k-1} - \cdots - a_k$ — первообразный полином по модулю 2, и предположим, что $X_0, \ldots, X_{k-1}$ — целые числа, не все четные.

a) Докажите, что длина периода последовательности, заданной рекуррентным соотношением $X_n = (a_1X_{n-1} + \cdots + a_kX_{n-k}) \bmod 2^e$, равна $2^{e-1}(2^k - 1)$ для всех $e \geq 1$ тогда и только тогда, когда $f(x)^2 + f(-x)^2 \not\equiv 2f(x^2)$ и $f(x)^2 + f(-x)^2 \not\equiv 2(-1)^k f(-x^2)$ (по модулю 8). [*Указание.* Равенство $x^{2^k} \equiv -x$ (по модулям 4 и $f(x)$) справедливо тогда и только тогда, когда $f(x)^2 + f(-x)^2 \equiv 2f(x^2)$ (по модулю 8).]

b) Докажите, что это условие всегда выполняется, когда полином $f(x) = x^k \pm x^l \pm 1$ является первообразным полиномом по модулю 2 и $k > 2$.

31. [*M30*] (Дж. Марсалья (G. Marsaglia).) Какова длина периода последовательности (7′), когда $m = 2^e \geq 8$? Предположите, что не все $X_0, \ldots, X_{54} \equiv \pm 1$ (по модулю 8).

32. [*M21*] Каким рекуррентным соотношениям удовлетворяют элементы подпоследовательностей $\langle X_{2n} \rangle$ и $\langle X_{3n} \rangle$, когда $X_n = (X_{n-24} + X_{n-55}) \bmod m$?

▶ **33.** [*M23*] (a) Пусть $g_n(z) = X_{n+30} + X_{n+29}z + \cdots + X_nz^{30} + X_{n+54}z^{31} + \cdots + X_{n+31}z^{54}$, где X_n удовлетворяют рекуррентному соотношению Фибоначчи с запаздыванием (7). Найдите простое соотношение между $g_n(z)$ и $g_{n+t}(z)$. (b) Выразите X_{500} в терминах $X_0, \ldots, X_{54}$.

34. [*M25*] Докажите, что обратная рекуррентная последовательность (12) имеет период $p + 1$ тогда и только тогда, когда полином $f(x) = x^2 - cx - a$ обладает следующими двумя свойствами: (i) $x^{p+1} \bmod f(x)$ равняется отличной от нуля константе, если вычислять, используя полиномиальную арифметику по модулю p; (ii) $x^{(p+1)/q} \bmod f(x)$ имеет степень 1 для каждого простого q, делящего $p + 1$. [*Указание.* Рассмотрите степени матрицы $\left(\begin{smallmatrix} 0 & 1 \\ a & c \end{smallmatrix}\right)$.]

35. [*HM35*] Как много пар (a, c) удовлетворяют условиям упр. 34?

36. [*M25*] Докажите, что обратная конгруэнтная последовательность $X_{n+1} = (aX_n^{-1} + c) \bmod 2^e$, $X_0 = 1$, $e \geq 3$, имеет период длиной 2^{e-1} всякий раз, когда $a \bmod 4 = 1$ и $c \bmod 4 = 2$.

▶ **37.** [*HM32*] Пусть p — простое число, и предположим, что $X_{n+1} = (aX_n^{-1} + c) \bmod p$ определяет обратную конгруэнтную последовательность с периодом $p + 1$. К тому же пусть $0 \leq b_1 < \cdots < b_d \leq p$. Рассмотрим множество

$$V = \{(X_{n+b_1}, X_{n+b_2}, \ldots, X_{n+b_d}) \mid 0 \leq n \leq p \text{ и } X_{n+b_j} \neq \infty \text{ для } 1 \leq j \leq d\}$$

В нем содержится $p + 1 - d$ векторов; любые d из них лежат в некоторой $(d - 1)$-мерной гиперплоскости $H = \{(v_1, \ldots, v_d) \mid r_1v_1 + \cdots + r_dv_d \equiv r_0 \text{ (по модулю } p)\}$, где $(r_1, \ldots, r_d) \not\equiv (0, \ldots, 0)$. Докажите, что никакие $d + 1$ векторов из V не лежат в одной и той же гиперплоскости.