Тут $[\cdot]$ — целая часть, а $\{\cdot\}$ — дробная.

Иная формула для последовательности фон Неймана такова:

$$\gamma_{n+1} = 10^{-2k}\left[10^{2k}\left\{10^{k}\gamma_n^2\right\}\right]. \tag{4}$$

4.2. Метод Ковэю. Метод Ковэю почти идентичен методу середины квадрата, однако гарантирует больший период. Пусть e — некоторое натуральное число. Выберем X_0 так, чтобы

$$2 \equiv X_0 \pmod 4.$$

Последовательностью Ковэю называется

$$X_{n+1} \equiv X_n(X_n + 1) \pmod{2^e}, \qquad n \geq 0. \tag{5}$$

Если, например, $e = 10$, и $X_0 = 13 \times 4 + 2 = 54$, то первые восемь членов последовательности Ковэю будут такими:

n	1	2	3	4	5	6	7	8
Z_n	2 , 970	851 , 006	3 , 906	696 , 390	4 , 970	764 , 750	716 , 562	618 , 582
X_{n+1}	922	62	834	70	874	846	786	86

В этой таблице мы обозначили $Z_n = X_n(X_n + 1)$.

4.3. Метод Фибоначчи. Простейший случай зависимости от более, чем одного из предыдущих значений реализуется *последовательностью Фибоначчи*:

$$X_{n+1} \equiv (X_n + X_{n-1}) \pmod m. \tag{6}$$

В настоящее время последовательность (6) не считается “*достаточно случайной*”.

4.4. Псевдослучайные числа. Числа, которые вычисляются рекуррентно по какой-либо заданной формуле, и впоследствии используются вместо случайных чисел, называются *псевдослучайными*. Таким образом, псевдослучайные числа вычисляются согласно рекурсии

$$\gamma_{n+1} = f(\gamma_n), \qquad n \geq 1. \tag{7}$$

Отметим, что все методы, описанные выше, генерируют псевдослучайные числа.

Начальное значение γ_0 выбирается так, чтобы последовательность $\{\gamma_n\}$ имитировала как можно больше свойств последовательности независимых случайных величин, имеющих равномерное распределение на отрезке $[0, 1]$.

Функция f имеет важнейшее значение для подобной процедуры. Например, выбор $f(x) = x$ совсем плох, так как все числа в (7) совпадают с начальным.

Одним из требований к f является такое: ее график должен как можно плотнее заполнять квадрат $[0, 1] \times [0, 1]$. Это требование объясняется таким свойством последовательности независимых равномерных случайных величин $\{r_n\}$: случайные векторы

$$(r_1, r_2), \quad (r_3, r_4), \quad (r_5, r_6), \quad \ldots \tag{8}$$

независимы и имеют равномерное распределение в квадрате $[0, 1] \times [0, 1]$. Это, в частности, означает, что если выбрать достаточно длинный фрагмент последовательности (8), то каждое подмножество квадрата ненулевой площади будет содержать элементы этого фрагмента.

Рассмотрим, например, функцию, график которой, изображен на рис. 4. Если выбрать $\gamma_0 = \frac{1}{4}$, то все точки

$$(\gamma_1, \gamma_2), \quad (\gamma_3, \gamma_4), \quad (\gamma_5, \gamma_6), \quad \ldots$$

будут находиться в квадрате $\left[0, \frac{1}{2}\right] \times \left[\frac{1}{2}, 1\right]$. Более того, последовательность $\{\gamma_n\}$ будет периодической: $\frac{3}{4}, \frac{1}{4}, \frac{3}{4}, \ldots$ и не может претендовать на роль псевдослучайной.

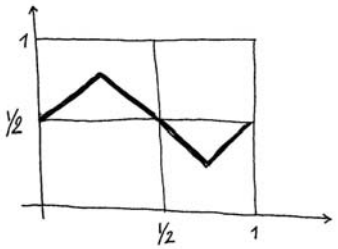

Рис. 4.

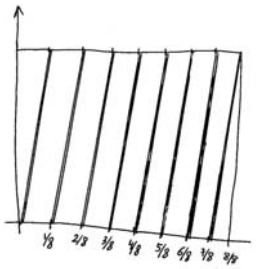

Рис. 5.

С такой ролью лучше справляется функция $f(x) = \{8x\}$, график которой изображен на рис. 5.

Еще лучшей будет функция $f(x) = \{cx\}$, если c — большое число.

5. Линейный конгруэнтный метод

Одним из свойств равномерного распределения является следующее: если Y — это равномерно распределенная на интервале $[0, 1]$ случайная величина, то

$$X = (kY + c) \bmod 1 \tag{9}$$

также равномерно распределенная на интервале $[0, 1]$ случайная величина. Тут k — натуральное число, $c \in \mathbf{R}$, а $\bmod 1$ — это взятие дробной части. Свойство (9) оказалось исключительно полезным при разработке датчиков псевдослучайных чисел.

В 1948 году американский математик Дик Лемер предложил простой метод генерации случайных чисел, основанный на арифметике по модулю. В методе Лемера каждое

число определяет следующее с помощью линейной функции и последующего вычисления остатка от деления. Хотя этот метод и дает лишь конечную последовательность, он и до сих пор служит основой для самых современных генераторов случайных чисел. Изучение метода Лемера попрежнему необходимо для понимания функционирования более сложных генераторов.

Линейный конгруэнтный метод Лемера основан на рекуррентном уравнении

$$x_i \equiv (ax_{i-1} + c) \pmod{m}. \tag{10}$$

Число a называется множителем, c — приращением, а m — модулем генератора. Довольно часто число c в (10) выбирают равным нулю. В этом случае метод называется *мультипликативным конгруэнтным*:

$$x_i \equiv ax_{i-1} \pmod{m}. \tag{11}$$

В качестве начального значения выбирается определенное число x_0. Последовательность, определяемая рекуррентным равенством (10), называется *последовательностью Лемера*. Каждое значение x_i можно масштабировать, чтобы оно принадлежало интервалу $(0, 1)$, с помощью деления на m, то есть рассматривая $u_i = x_i/m$.

Если a и m выбраны подходящим образом, то последовательность $\{u_i\}$ будет "выглядеть" похожей на последовательность значений случайных величин, имеющих равномерное распределение на интервале $[0, 1]$.

Рекуррентное уравнение (11) для целых чисел эквивалентно такому уравнению для чисел из отрезка $[0, 1]$:

$$u_i \equiv au_{i-1} \pmod{1}. \tag{12}$$

Замечание 4. Сам Лемер использовал константы $a = 23$, $m = 10^8 + 1$. Датчик вида (10) с $c \neq 0$ впервые описан Ротенбургом в 1960 году. Последовательность Ротенбурга отвечает параметрам $a = 2^7$, $c = 1$, $m = 2^{35}$.