Триша Тройкин, Петя Пятаков и Сёма Семак пытаются сконструировать собственный генератор псевдослучайных чисел.

Для этого они взяли натуральные числа a и m (одни и те же у всех троих) и выстраивают последовательность по правилу:

$$x_{n+1} = x_n a \ (mod\ m).$$

Начав с некоторого x_1, Триша посчитал x_2, x_3 и x_4. Но x_4 оказалось равно x_1.

Тогда он взял другое (не встречавшееся ранее) число в качестве x_1. Но последовательность опять зациклилась на третьем шаге. Треья попытка привела Тришу к тому же результату.

Петя совершил пять попыток подобрать x_1. Но всякий раз получал новые циклы длины 5.

Наиболее упорным оказался Сёма. Он совершил семь попыток. И получил семь циклов длины 7.

При каком наименьшем m могла возникнуть такая ситуация?

РЕШЕНИЕ

Умножение на фиксированное натуральное число с последующим приведением по модулю m задает на множестве классов вычетов по модулю m отображение в себя, т. е. структуру унара (множества с одной унарной операцией). Назовем класс b циклическим, если найдется натуральное n такое, что $ba^n \equiv b \ (mod\ m)$ (1). Наименьшее натуральное n, при котором выполняется сравнение (1) назовем периодом элемента b.

Обозначим: $d = (a, m) = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}$, $P = p_1 p_2 \ldots p_3$.

Тогда $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} a', m = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k} m'$,

$b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k} b'$, где $(a', P) = (m', P) = (b', P) = 1$,

a_i, m_i - натуральные, b_i -целые неотрицательные.

Пусть, далее, $mm = m'/(m', b)$, $T(b)$ - период b.

Доказательства следующих лемм почти очевидны.

Лемма 1.

b - циклический тогда и только тогда, когда $b_i \geq m_i$ для всех i.

Лемма 2.

$T(b) = ord_{mm}(a)$, т.е. порядку a по модулю mm.

Применительно к нашей задаче это означает, что m должно содержать минимум три попарно взаимно простых сомножителя, значения функции Эйлера от которых должны делиться на 3, 5 и 7 соответственно (чтобы после умножения на разные b получились три соответствующих порядка у одного и того же a по возникающим модулям mm).

Наименьшими такими сомножителями будут числа 7, 11 и 29.

Подобрав a, сравнимое с элементами порядков 3, 5 и 7 по этим модулям, получим на множестве классов вычетов по модулю m_0 = 7·11·29 унар, содержащий циклы длин 3, 5 и 7.

Однако m_0 не годится в качестве m. В самом деле, $\frac{\varphi(7)}{3} = 2$, $\frac{\varphi(11)}{5} = 2$ и $\frac{\varphi(29)}{7} = 4$. Потому при подходящем a будут возникать всего 2 цикла длины 3, 2 цикла длины 5 и 4 цикла длины 7. ($\varphi(n)$ - функция Эйлера).

Увеличивать количество циклов данных длин можно разными путями:

1. Заменить числа 7, 11 и 29 на бОльшие простые таким образом, чтобы значения функции Эйлера этих чисел по-прежнему делились на 3, 5 и 7 соответственно. Этот способ не слишком экономичен. В самом деле, замена 7 на 13 увеличить до 4 количество циклов длины 3, но не добавит циклов длин 5 и 7.

Поэтому наименьшим подходящим m, полученным таким способом будет $m = 13 \cdot 31 \cdot 71 = 28613$. При a, равном, например, 250, в соответствующем унаре будет $\frac{\varphi(13)}{3} = 4$ циклов длины 3, $\frac{\varphi(31)}{5} = 6$ циклов длины 5 и $\frac{\varphi(71)}{7} = 10$ циклов длины 7.

2. Домножить найденное m_0, на некоторый множитель. В этом случае необходимо позаботиться о том, чтобы порядок числа a по модулую этого множителя был равен 1 (чтобы не изменились длины циклов, а лишь возросло их количество).

Наименьшим подходящим множителем будет число 3, поскольку $2\varphi(11)/5 = 4$ и циклов длины 5 будет все еще недостаточно.

Такой подход даст $m = 3 \cdot 7 \cdot 11 \cdot 29 = 6699$. При $a = 16$ в соответствующем унаре будет $3\varphi(7)/3 = 6$ циклов длины 3, $3\varphi(11)/5 = 6$ циклов длины 5 и $3\varphi(29)/7 = 12$ циклов длины 7.

3. Заменить числа 7, 11, 29 (или некоторые из них) на 9, 25, 49, значения функции Эйлера которых, тоже кратны 3, 5 и 7 соответственно.

Поскольку $\varphi(9) = 6 = 2 \cdot 3$ так же как и $\varphi(7)$, этот подход не увеличит количества циклов длины 3 при замене $m = 7 \cdot 11 \cdot 29$ на $m = 9 \cdot 11 \cdot 29$.

Зато замена 7 на 9 позволяет утроить количество циклов длин 5 и 7. Ведь теперь Пятакову достаточно в качестве начальных выбирать числа кратные 29 и 3 (а не 9), поэтому его m'' будет равно $11 \cdot 3$.

Точно так же, при начальных числах кратных 11 и 3, m'' Семака будет равно $29 \cdot 3$.

Аналогичным образом замена в m_0 множителя 11 на 25 позволить упятерить количество циклов длин 3 и 7, а замена 29 на 49 увеличить в 7 раз число циклов длин 3 и 5.

Этот подход позволяет получить сразу несколько m, меньших $3 \cdot 7 \cdot 11 \cdot 29$ и удовлетворяющих условиям задачи:

$m = 9 \cdot 25 \cdot 29 = 6525$. В качестве a вновь подходит число 16. А в соотвествующем унаре будет $5\varphi(9)/3 = 10$ циклов длины 3, $3\varphi(20)/5 = 12$ циклов длины 5 и $3 \cdot 5 \cdot \varphi(29)/7$ = 60 циклов длины 7;

$m = 9 \cdot 11 \cdot 49 \ = 4851$. В качестве a можно взять число 169. А в соответствующем унаре будет $7\varphi(9)/3 \ = \ 14$ циклов длины 3, $7 \cdot 3\varphi(11)/5 \ = \ 42$ цикла длины 5 и $3\varphi(49)/7 \ = 18$ циклов длины 7.

4. Скомбинироать предыдущие способы.

Наименьшим m, полученным таким путем будет $m \ = 2 \cdot 9 \cdot 11 \cdot 29 \ = 5742$. В качестве a можно взять число 25. А в соответствующем унаре будет $2\varphi(9)/3 \ = 4$ цикла длины 3, $2 \cdot 3\varphi(11)/5 = 12$ циклов длины 5 и $2 \cdot 3\varphi(29)/7 = 24$ цикла длины 7;

Однако это значение m больше предыдущего.

Ответ: $m \ = \ 4851$.