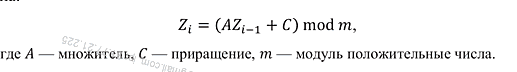
**27.           Расскажите о конгруэнтном генераторе с простым модулем и о механизме избежать явного деления по модулю.**

**Линейный конгруэнтный метод** — один из методов генерации случайных чисел. Основными операциями являются операции умножения и взятия остатка от деления. В линейном конгруэнтном генераторе для получения числа Zi из предыдущего используется следующая рекурсивная формула:



Количество неповторяющихся цифр в цикле (длина цикла) называется периодом генератора. Числа Zi могут принимать m возможных значений (целые от 0 до m-1). Потом получают случайное число Ui принадлежащее [0,1), делят остаток от деления на модуль m.



Если период генератора содержит все такие числа, период генератора равен m, то говорят, что такой генератор имеет полный период.

Теорема(Халл и Добелл)

Линейный конгруэнтный генератор имеет полный период тогда и только тогда, когда выполняются следующие условия:

1. Параметры C и m являются взаимно простыми (наибольший общий делитель=1)
2. Число A-1 должно делиться на все простые числа, из произведения которых состоит модуль m
3. Если модуль m делится на 4, то A-1 тоже должно делиться на 4

В ЛКГ операция взятия остатка от деления mod является трудоемкой. Чтобы генератор работал быстро, существует приём, позволяющий избежать явного деления по модулю

Переполнение разрядной сетки

Берем модуль m как минимально возможное число в компьютерной слове. Если в машинном слове 32 бита и 1 бит-знак, то максимально возможный модуль m=232

Переполнение разрядной сетки: все биты, которые не влезли в разрядную сетку, будут отброшены, а то, что останется-результат остатка от деления

**Генератор с простым модулем**

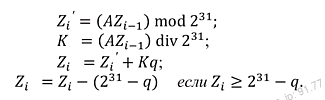
У таких генераторов параметр C=0, поэтому теорема о полном периоде не выполняется, они не могут обладать полным периодом.(период<m). Если взять модуль m=232 , то период составит максимум одну четвертую 232-2

Если брать простой модуль (простое число), то модуль будет m-1. Период неполный, но разница минимальная. Множитель A нужен такой, чтобы Аm-1 делилось на модуль m (А-первообразный элемент по модулю m)

Так как мы уменьшили m, механизм переполнения не помогает избежать операции деления.

Пусть наш модуль m=231-q(у нас q=1) Воспользуемся приемом с переполнением для 31 разряда.

K-целая часть от деления по модулю m. За каждую 1 в целой части от деления на m, мы недополучаем в остатке число q. Значит к K нужно прибавить q. Но после прибавления возможен выход за разрядную сетку, в этом случае надо отнять число 231-q



Нужно подобрать А такое, чтобы статистические свойства генератора были наилучшими. Фишман и Мур выявили, что А должен быть 630360016

Итог: проверенным и хорошим линейным конгруэнтным генератором случайных чисел является генератор с простым модулем m=231-q и множителем А=630360016