**Постановка задачи**

1. Разработайте программу (улититу) для создания и исследования *линейных конгруэнтных генераторов* (ЛКГ). Требования к утилите приводятся далее по тексту.  
2. Создайте и исследуйте несколько ЛКГ с указанными в задании характеристиками. Результаты исследования приведите в отчете. План исследования приводится далее по тексту.

**Требования к утилите**

Программа должна считывать **одну команду** из файла *input.txt* и выводить результаты вычисления в файл *output.txt*.  
Команда состоит из ключевого слова и списка аргументов. Аргументы отделены от ключевого слова и друг от друга **одним или несколькими пробелами**. **Порядок следования аргументов** жестко не регламентируется и **может быть любым**. Длина строки с командой не регламентирована, строка может быть **сколь угодно длинной**.  
  
В реализации программы необходимо обойтись **без вызова функций динамического управления памятью (malloc, calloc, free)**.  
  
Должны поддерживаться следующие команды со следующими аргументами:  
  
**get\_c cmin=ЧИСЛО cmax=ЧИСЛО m=ЧИСЛО** - подобрать все c - взаимно простые с m. 0 < c < m; cmin <= c <= cmax  
  
**get\_a m=ЧИСЛО** - подобрать минимальное a такое что, a-1 делится на все простые делители m. Если m делится на 4 то и a-1 делится на 4;  
0 < a < m, m <= 18446744073709551615 (264-1). Результат выводится в выходной файл. Если не найдено решения - вывести 'no solution'   
  
**lcg a=ЧИСЛО x0=ЧИСЛО c=ЧИСЛО m=ЧИСЛО n=ЧИСЛО** - сгенерировать n чисел с помощью указанного ЛКГ. Результат вывести в файл, по одному числу на строке.   
0 <= a,x0,c,m,n <= 18446744073709551615 (264-1); a,x0,c < m. Вывести 'no solution' если вычисления невозможны (например, n=0, или a,c,x0 >= m).   
  
**bits a=ЧИСЛО x0=ЧИСЛО c=ЧИСЛО m=ЧИСЛО n=ЧИСЛО** - сгенерировать n чисел с помощью указанного ЛКГ. Для каждого из битов сгенерированных чисел проверить - установлен он или нет. В результирующий файл вывести 64 числа по одному на строке: каждая строка содержит количество чисел, выданных ЛКГ, у которых был установлен соответствующий бит. Значение в строке может быть от 0 до n. Значение близкое к n/2 свидетельствует о том, что поведение бита может быть похоже на случайное (Частотный побитовый тест). Строки выводятся в порядке от старшего бита к младшему (первая строка - значение для старшего бита, последняя строка - для младшего)  
0 <= a,x0,c,m,n <= 18446744073709551615 (264-1); a,x0,c < m. Вывести 'no solution' если вычисления невозможны.   
  
**Иначе**, если команда нераспознана, либо были указаны не все аргументы, либо аргументы указаны некорректно (например, отрицательные числа или буквы в значении аргумента), то в output.txt должно быть выведено **incorrect command**. 

**Исследование генераторов**

Проведите исследование ЛКГ по приведенному ниже алгоритму.  
1.1. Возьмите любое число m, такое что m - простое, размер m - **?? бит(а)**.  
1.2. Возьмите любое c, 0 < c < m.   
1.3. Возьмите любое a, 0 < a < m, такое, что а-1 - простое.  
1.4. Вычислите перод полученного ЛКГ для различных x0 (не менее 5). Возьмите разные x0, идущие подряд, например 1,2,3,4,5.  
В отчете опишите **способ определения периода** ЛКГ. Сравните ваш результат с теоремой о ЛКГ. Объясните полученный результат.  
1.5. Вычислите вероятности выпадения значений битов для полученной псевдослучайной последовательности, используя вашу утилиту. Для оценки используйте команду bits со значением n=10000. Приведите результаты работы утилиты. Сделайте выводы о том - какие биты ведут себя случайно, а какие - нет.  
  
2. Возьмите m такое, что m - произведение нескольких (не менее 10) простых множителей, размер m - ?? бит(а).  
Используя утилиту подберите c такое, что c - взаимно просто с m. В отчете представьте полученный утилитой вывод.  
Возьмите a - такое, чтобы удовлетворяло условию теоремы о макс. периоде ЛКГ. Подбирайте a с помощью утилиты. В отчете представьте полученный утилитой вывод.  
Оцените период для 5 различных x0 (как в п. 1.4), сделайте выводы о соответствии полученного периода с теоремой о ЛКГ.  
Выявите номера битов ведущих себя случайно (как в п. 1.5).   
Вычислите мощность полученного генератора.  
Объясните - является ли полученный генератор "хорошим"? Если нет, то что и как надо изменить чтобы он стал "хорошим"?   
  
3. Возьмите ваши m и c из п.2. Возьмите a такое, что a-1 - составное, но **НЕ удовлетворяет** условию теоремы о макс. периоде ЛКГ.  
Проведите исследования периода и случайности битов по плану п.1.  
  
4. Возьмите m и a из п. 2. Возьмите c такое, что c - **НЕ взаимно простое** с m.  
Проведите исследования периода и случайности битов по плану п.1.  
  
5. Возьмите m из п.2, a - из п.3, с - из п. 4.  
Проведите исследования периода и случайности битов по плану п.1.  
  
  
Заполните таблицу:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **N пп.** | **m** | | | **c** | | **a-1** | | **x0** | **Период** | **Выводы о периоде, мощность** | **Выводы о случ.битов** |
| **дес.** | **двочн.** | **прост.множ.** | **дес.** | **прост.множ.** | **дес.** | **прост.множ.** |
| 1. |  |  |  |  |  |  |  |  |  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 2. |  |  |  |  |  |  |  |  |  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 3. |  |  |  |  |  |  |  |  |  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 4. |  |  |  |  |  |  |  |  |  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 5. |  |  |  |  |  |  |  |  |  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |

*Примечания:* В таблице приведите представление m **в десятичном и в двоичном виде**.   
Приведите для m, c и a-1 все их **простые множители** (для случаев когда m, c и a-1 - составное число). 

**Содержание отчета**

* 1. Цели работы.
* 2. Описание задачи.
* 3. Алгоритмы и методы. В разделе приведите описание алгоритмов и методов, которые были вами применены при решении задачи (разработке программы).
* 4. Тестовые данные. Описание тестовых ситуаций (входных данных) и полученных выходных данных, которые были вычислены вашей программой. Требуется привести не менее 10 тестов для каждого из подзаданий. Программа должна быть проверена на каждом из тестов.
* 5. Выводы. Описание полученных вами в ходе выполнения работы знаний, умений и навыков. Описание трудностей, которые были встречены в работе, совершенных ошибок и способов их устранения.
* 6. Исследования ЛКГ - проведенные вами исследования согласно плану раздела "Исследование генераторов" исходного задания.  
  Необходимо описать:  
  - Способ определения периода ЛКГ.  
  - Результаты запуска (вывод программы) для команд get\_a и get\_c (для тех подпунктов, где это требовалось).  
  - Результаты запуска (вывод программы) для команды bits для каждого из подпунктов.  
  - Результирующая таблица, содержащая значения для m, c, a-1 и выводы о периоде и случайности битов. Для генератора с максимальным периодном необходимо вычислить мощность и указать результаты ваших исследований о том, является ли генератор "хорошим" и/или как его можно сделать таковым.
* 7. Текст программы.