ЗАДАНИЕ 9. Метод пробного деления (разложение числа на простые множители):

1. Создание базы данных из произведений простых чисел.

Вход: файл базы данных простых чисел; параметр t (число простых множителей).

Выход: файл базы данных из произведений по t простых чисел.

2. Метод пробного деления.

Вход: натуральное число; файл базы данных из произведений простых чисел.

Выход: файл разложения натурального числа на простые множители.

ЗАДАНИЕ 10. ρ-метод Полларда (разложение числа на простые множители):

Вход: 1) Число n — нечётное число.

2) Начальное значение c: $1 < c < n$.

3) Функция f, обладающая сжимающими свойствами, например, $f(x) \equiv x^2 + 1 \pmod{n}$.

Выход: Нетривиальный делитель p числа n.

Алгоритм

1. Положим $a \leftarrow c$, $b \leftarrow c$.
2. Вычислить $a \leftarrow f(a) \pmod{n}$,
   $b \leftarrow f(b) \pmod{n}$,
   $b \leftarrow f(b) \pmod{n}$.
3. Найти $d \leftarrow$ НОД$(a - b, n)$.

Если $1 < d < n$, то положить $p \leftarrow d$ и результат: p. При $d = n$ результат: «Делитель не найден». При $d = 1$ вернуться на шаг 2.

Примеры и обоснование см. лекции.

ЗАДАНИЕ 11. ($p - 1$)-метод Полларда (разложение числа на простые множители):

Вход: 1) Число n — нечётное число;

2) Файл базы данных простых чисел.

Выход: Нетривиальный делитель p числа n.

Алгоритм

1. Выбрать базу разложения $B = \{p_1, p_2, \ldots, p_s\}$.
2. Выбрать случайное целое a, $2 \le a \le n - 2$, и вычислить $d \leftarrow$ НОД(a, n). При $d \ge 2$ положить $p \leftarrow d$ и результат: p.
3. Для $i = 1, 2, \ldots, s$ выполнить следующие действия.

   3.1. Вычислить $l \leftarrow \left[\dfrac{\ln n}{\ln p_i} \right]$.

   3.2. Положить $a \leftarrow a^{p_i^l} \pmod{n}$.
4. Вычислить $d \leftarrow$ НОД$(a - 1, n)$.
5. При $d = 1$ или $d = n$ результат: «Делитель не найден». В противном случае положить $p \leftarrow d$ и результат: p. □

Примеры и обоснование см. лекции.

ЗАДАНИ 12. Метод квадратов (метод Ферма):
Вход: n — большое натуральное число,

k — небольшое натуральное число, коэффициент близости, примерные значения $k \in \{1, 2, 3, 4, \ldots, 10, ..\}$.

l — натуральное число — число итераций.

Выход: p— простой делитель числа n.

Задача: Последовательно вычисляем $s = [\sqrt{kn}] + i$, $i = 1,2,3....$ пока не найдётся такое s, что разность $s^2 - kn$ является полным квадратом, т.е. $s^2 - kn = t^2$. Тогда НОД(kn, $s - t$) = p.

Чтобы программа не зависала на неопределённое время, сделать после $i = l$ сообщение «прошло l вычислений. Осуществить следующие l вычислений: Y/N», и т.д.

https://drive.google.com/open?id=0B2AKc7ibPQ_WY1dMbWVVbFJVbkk