**Алгоритм Шенкса**

Пусть задано сравнение , необходимо найти натуральное число , удовлетворяющее данному сравнению.

Алгоритм реализован следующим образом:

1) Сначала берутся два целых числа и , такие, что . Как правило .

2) Вычисляются два ряда чисел:

,

.

Все вычисления проводятся по модулю .

3) Идёт поиск таких и , для которых выполняется равенство . То есть ищется во втором ряду такое число, которое присутствует и в первом ряду. Запоминаются показатели степени и , при которых данные числа получались.

4) В результате работы алгоритма неизвестная степень вычисляется по формуле .

**Алгоритм Полига-Хеллмана**

Пусть задано сравнение , необходимо найти натуральное число , удовлетворяющее данному сравнению.

Шаги выполнения алгоритма:

1) Идёт разложение числа на простые множители.

2) Составляется таблица значений ,

где .

3) Вычисляется .

Для от 1 до :

Пусть ,

где .

Тогда верно сравнение:

.

С помощью таблицы, составленной на шаге 1, находится .

Для от 0 до рассматривается сравнение

.

Решение находится по таблице

Конец цикла по .

Конец цикла по .

4) Найдя для всех , происходит поиск

по китайской теореме об остатках.

**Ро-метод Полларда**

Шаги выполнения алгоритма:

1) Вычисляются тройки чисел

.

Причём каждая такая тройка получается из предыдущей.

2) Каждый раз, когда число кратно , вычисляется наибольший общий делитель любым известным способом.

3) Если , то частичное разложение числа найдено, причём . Найденный делитель может быть составным, поэтому его также необходимо факторизовать. Если число составное, то продолжаем алгоритм с модулем .

4) Вычисления повторяются раз. Если при этом число не было до конца факторизовано, выбирается, например, другое начальное число .

**Алгоритм Адлемана**

Пусть задано сравнение , необходимо найти натуральное число , удовлетворяющее данному сравнению.

Описание алгоритма:

1) Сформировывается факторная база, состоящая из всех простых чисел :

.

2) С помощью перебора идёт поиск натуральных чисел таких, что

,

то есть раскладывается по факторной базе. Отсюда следует, что .

3) Набрав достаточно много соотношений из 2 шага, решается получившаяся система линейных уравнений относительно неизвестных дискретных логарифмов элементов факторной базы .

4) С помощью некоторого перебора ищется одно значение , для которого , где – простые числа «средней» величины, то есть , где – также некоторая субэкспоненциальная граница, .

5) С помощью вычислений, аналогичных этапам 2 и 3 ищутся дискретные логарифмы .

6) Определяется искомый дискретный логарифм:

.

**Алгоритм COS**

Пусть задано сравнение , необходимо найти натуральное число , удовлетворяющее данному сравнению.

Описание алгоритма:

1) Задаётся . Сформировывается множество , где и – простые величины, .

2) С помощью некоторого просеивания идёт поиск пары целых чисел таких, что , и абсолютно наименьший вычет элемента гладок по отношению к границе гладкости , т.е.

.

При этом, поскольку , то

, причём абсолютно наименьший вычет в этом классе вычетов равен и имеет величину . Поэтому вероятность его гладкости выше, чем для произвольных чисел на отрезке . Логарифмируя по основанию , получается соотношение

*.*

Это однородное уравнение относительно неизвестных величин . Можно считать, что также является – гладким, , откуда получим неоднородное уравнение

*.*

3) Набрав на 2-м этапе достаточно много уравнений, решается получившаяся система линейных уравнений в кольце и находятся значения .

4) Для нахождения конкретного логарифма мы введём новую границу гладкости . Случайным перебором находим одно значение такое, что

.

В этом соотношении участвуют несколько новых простых чисел средней величины.

5) С помощью методов, аналогичных 2 и 3 этапам, мы находим логарифмы нескольких простых чисел средней величины, возникших на 4 этапе.

6) Находим ответ

.

**Решето числового поля**

Пусть задано сравнение , необходимо найти натуральное число , удовлетворяющее данному сравнению.

Описание алгоритма:

1) Пусть — нечетное составное число, которое требуется факторизовать.

2) Выберем степень неприводимого многочлена (при не будет выигрыша в сравнении с методом квадратичного решета).

3) Выберем целое такое, что , и разложим по основанию :

.

4) Свяжем с разложением из 3 шага неприводимый в кольце полиномов с целыми коэффициентами многочлен

.

5) Определим полином просеивания как однородный многочлен от двух переменных и :

.

6) Определим второй полином и соответствующий однородный многочлен .

7) Выберем два положительных числа и , определяющих область просеивания:

.

8) Пусть  — корень . Рассмотрим кольцо полиномов . Определим множество, называемое алгебраической факторной базой , состоящее из многочленов первого порядка вида с нормой шага 5, являющейся простым числом. Эти многочлены — простые неразложимые в кольце алгебраических целых поля . Ограничим абсолютные значения норм полиномов из константой

9) Определим рациональную факторную базу , состоящую из всех простых чисел, ограниченных сверху константой .

10) Определим множество , называемое факторной базой квадратичных характеров. Это множество полиномов первого порядка , норма которых - простое число. Должно выполняться условие .

11) Выполним просеивание многочленов по факторной базе и целых чисел по факторной базе . В результате получим множество , состоящее из гладких пар , то есть таких пар , что НОД= 1, полином и число и раскладываются полностью по и соответственно.

12) Найдём такое подмножество , что

.

13) Определим многочлен

, где – производная .

14) Многочлен является полным квадратом в кольце полиномов . Пусть тогда есть корень из и — корень из .

15) Строим отображение , заменяя полином числом . Это отображение является кольцевым гомоморфизмом кольца алгебраических целых чисел в кольцо , откуда получаем соотношение:

.

16) Пусть . Найдём пару чисел таких, что . Тогда найдём делитель числа , вычисляя НОД.