Факторизация чисел Ро-методом Полларда

Кузнецова Арина 6373

Ро-алгоритм Полларда

В 1975 году Поллард опубликовал статью, в которой он, основываясь на алгоритме обнаружения циклов Флойда, изложил идею алгоритма факторизации чисел, работающего за время, пропорциональное $N^{1/4}$.

С его помощью было разложено на множители число Ферма $F_8 = 2^{256} + 1$.

Оригинальная версия алгоритма

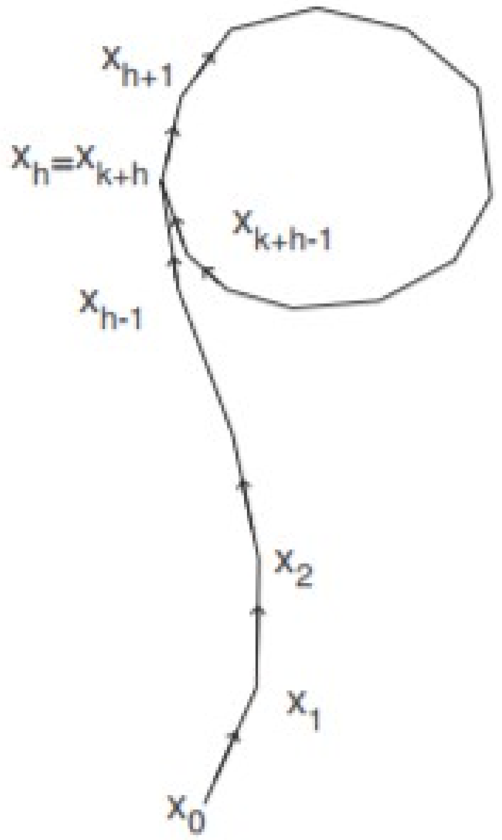
Возьмем некоторое случайное отображение

$f : Z_n \to Z_n$, которое сгенерирует некоторую случайную последовательность x0, x1, x2, . . . где $x_i = f(x_{i-1})$. Обычно берётся многочлен f(x) = x*x + 1.

Функция f имеет не более, чем n значений, поэтому последовательность зациклится.

$x_{k+h} = x_h$

h называется индексом вхождения, k - длиной цикла.



Оригинальная версия алгоритма

Рассмотрим теперь алгоритм подробнее.

При выбранном многочлене $F(x) = x*x + 1 \pmod n$ рассматриваем две последовательности чисел:

$x_0 = 0, x_1 = 1, \ldots, x_{n+1} = F(x_n)$,

$y_0 = 1, y_1 = 5, \ldots, y_{n+1} = F(F(y_n))$

и для всех n вычисляем НОД $d = \gcd(x_n, y_n)$.

Если $d > 1$, то d – нетривиальный делитель n.

Если n/d - составное число, то применяем данный алгоритм ещё раз уже к числу n/d. И так продолжаем до тех пор, пока не получим разложение только из простых чисел.

Особенности использования алгоритма

Следует отметить, что рассматриваемый алгоритм в значительной степени случаен, его эффективность сильно и непредсказуемо зависит от выбора многочлена и начального элемента в последовательности.

Метод эффективен для нахождения небольших простых делителей числа n. Делители большего размера тоже могут быть обнаружены, однако лишь с некоторой вероятностью.