ро-Алгоритм Полларда

Gagik T. Papikyan

RUDN University, Moscow, Russian Federation

ро-Алгоритм Полларда

Введение

Ро-алгоритм — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. Данный алгоритм основывается на алгоритме Флойда поиска длины цикла в последовательности и некоторых следствиях из парадокса дней рождения. Алгоритм наиболее эффективен при факторизации составных чисел с достаточно малыми множителями в разложении. Сложность алгоритма оценивается как O(N^{1/4})

Алгоритм

```
int Rho-Поллард (int N)
{
  int x = random(1, N-2);
  int y = 1; int i = 0; int stage = 2;
  while (Н.О.Д.(N, abs(x - y)) == 1)
  {
    if (i == stage){
      y = x;
      stage = stage*2;
    }
    x = (x*x + 1) (mod N);
    i = i + 1;
  }
  return Н.О.Д(N, abs(x-y));
}
```