Factorization methods analysis

Bereczki Norbert Cristian

December 14, 2017

1 Methods

1.1 Primitive algorithm

For i in the range 2,...,n/2 try to see if i|n. If yes then break. Elsewhere continue on.

1.2 Pollard's p algorithm

Let

$$x_0 = 2.$$

For j = 1, 2, . . . compute the sequence:

$$x_j = f(x_j - 1) \pmod n$$

and

$$d = (|x_{2j} - x_j|, n).$$

If 1 < d < n, then STOP and d is a non-trivial factor of n. If d = n, then STOP and FAILURE. In this case, one can repeat the algorithm with a different x0 or f . Else, continue with the next value of j.

2 Runtime analysis

Input	Primitive Algo	Pollard's p
911352783367	0	100
163398410325	0	0
623926552581	0	0
314047195607	0	0
849257520909	0	0
806442382101	0	0
125200496397	0	0
130417715505	0	0
1000119529	0	2
833837197611	0	0
10000001400000049	1074	doesn't stop