1 Problem statement

Implement the classical algorithm for factoring integers and Pollard's p - 1 algorithm.

Do a running time analysis of the two algorithms.

2 Algorithms

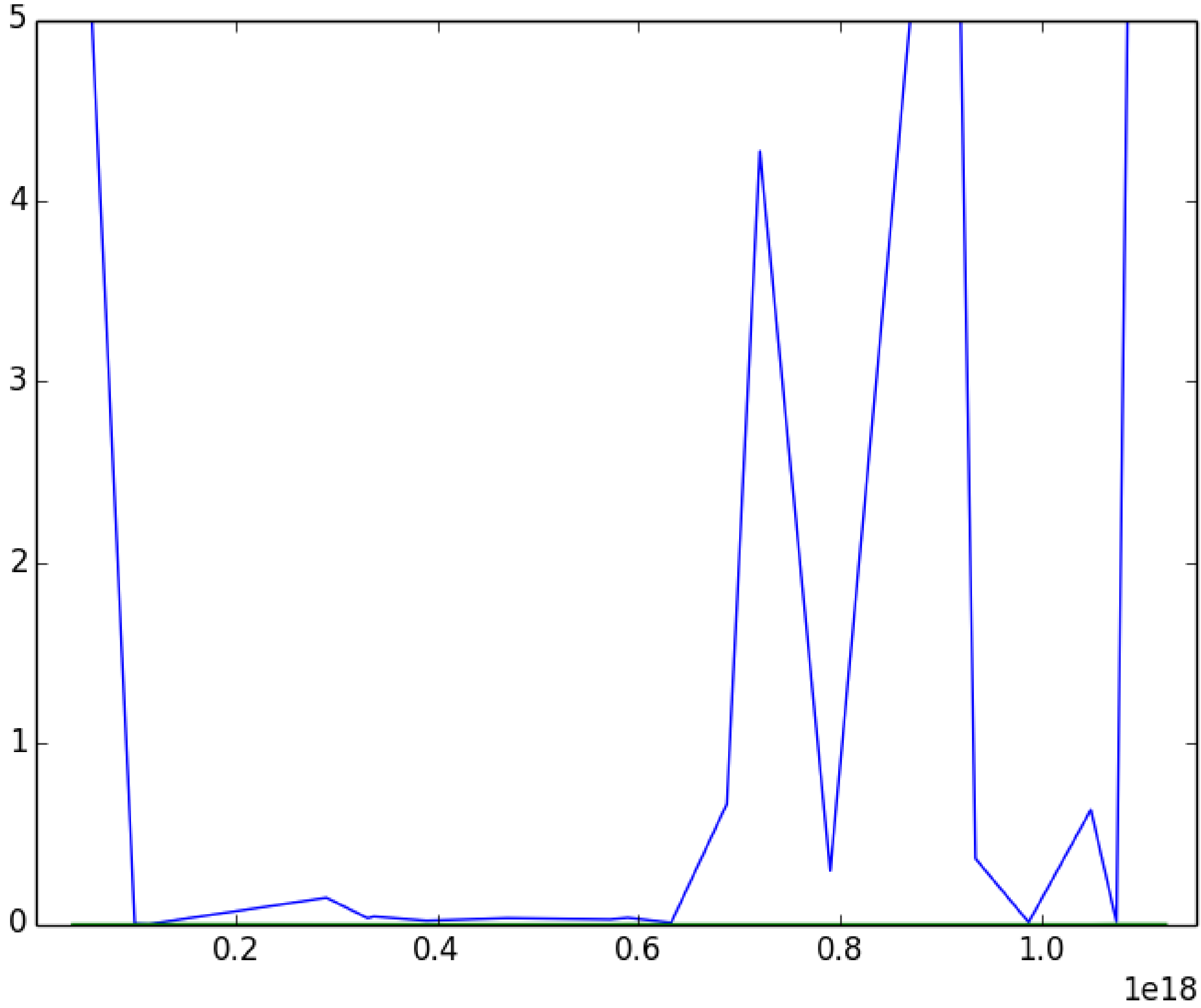
2.1 Trial division

procedure TRIAL(a)
  for $i = 2, \sqrt{n}$ **do**
    if $a \mod i = 0$ **then**
      trial ← i
    end if
  end for
end procedure

2.2 Pollard's p - 1

procedure POLLARD(n, b)
  k ← $lcm(1, ..., b)$
  a ← $random(1, n - 1)$
  a ← $a^k \mod n$
  d ← $gcd(a - 1, n)$
  if d=1 or d = n **then**
    trial ← n
  else
    trial ← d
  end if
end procedure

3 Runtime analysis



As can be seen from the graph, the naive, brute-force algorithm has an exponential complexity when the numbers are primes, or have only large divisors. Pollard's p-1 method is very fast, but it doesn't find all factors.