GCD Algorithms

Bereczki Norbert Cristian

November 16, 2017

Abstract

A composite natural number n is called a *Carmichael number* if $b^{n-1} = 1(mod n)$ (1) holds $\forall b \in Z$ with (b,n) = 1 .

1 Problem

Implement an algorithm for determining all Carmichael numbers less than a given bound.

2 Algorithm used

2.1 Brute force

For each x from 3 to Upper Bound check if it is composite, then iterate (with i) through 2 to x and check if gcd(x,i)=1 and that (1) holds.

2.2 Smart way

Used the following properties: If n is square free (that is, it is not divisible by the square of any prime), then n is a Carmichael number $\iff$ p-1|n-1 $\forall p$ prime that p|n.

First we precompute the Sieve of Eratosthenes up to the given upper bound. Given an upper bound iterate through all values x from 3 to the upper bound. If x is even we skip over it. We check if any of it's divisors is prime, and if it is we check that each prime divisor obeys: p-1 | n-1. Then we check that the number is squarefree by iterating through all prime numbers in the sieve until $[\sqrt{x}]$. If all is true until now then the x is a Carmichael number.