Finding primes like Édouard Lucas

2WF40 Writing Assignment Homework Group 14

Jan Bulthuis
Student Nr. 1696866
Eindhoven University of Technology

Lars van Dartel
Student Nr. 1673858
Eindhoven University of Technology

Stefan Engbers
Student Nr. 1757962
Eindhoven University of Technology

Wouter Vermeer
Student Nr. 1672428
Eindhoven University of Technology

October 26, 2021

Contents

1 Introduction

There are many useful application of large primes. One of them is the secure encryption of data using the cryptosystem RSA. For this, 2048-bit numbers are commonly used. Needless to say, with the amount of online traffic, the demand for large primes is enormous. However, primes much larger than 2048 bits (617 digits) long have very little use. Nonetheless, many people (or their computers) have spent thousands of hours computing primes as large as possible.

1.1 Mersenne primes

Mersenne primes are defined as prime numbers that are one less than a power of two, or formally $M_n = 2^n - 1$ for some $n \in \mathbb{N}$.

Statement. For $2^n - 1$ to be prime, n must be prime.
Proof. We use the identity:

$$X^{ab} - 1 = (X^a - 1) \cdot \left(X^{a(b-1)} + X^{a(b-2)} + ... + X^a + 1\right). \tag{1}$$

This tells us that if n is composite, i.e., $n = a \cdot b$ for some integers a and b, then $2^n - 1$ is also composite, since by the identity (1), $2^{ab} - 1$ can be factored into the factors $X^a - 1$ and $2^{a(b-1)} + 2^{a(b-2)} + ... + 2^a + 1$

1.2 Édouard Lucas

François Édouard Anatole Lucas (1842 - 1891) was a famous mathmetician that studied the Fibonacci sequcence. He devised his own method for checking the primality of large numbers without factorising. Using the Lucas numbers, which are much alike the Fibonacci sequcence. The Lucas numbers are defined in the following way:

$$\begin{aligned} L_1 &= 1; \\ L_2 &= 3; \\ L_n &= L_{n-1} + L_{n-2}. \end{aligned}$$

An integer n is *probably* prime, also called a Lucas probable prime, if $p \mid L_n$.

Lucas spent 19 years of his life proving the primality of the Mersenne prime $2^{127} - 1$. This still remains as the largest prime number of which the primality was proved by hand.

1.3 Lucas-Lehmer primality test

The primality test used by Lucas was later improved by the American mathmetician D.H. Lehmer. The primality of Mersenne number $M_p = 2^p - 1$ with p prime can be found in the following way:

Denote the sequence s by

$$\begin{aligned} s_1 &= 4; \\ s_n &= s_{n-1}^2 - 2, \end{aligned}$$

The first few elements of this sequence are $4, 14, 194, 37634, \ldots$.

then M_p is prime if and only if $s_{p-1} \equiv 0 \mod p$. The proof of this can be found here [Bruce, 1993].

2 Finding primes

There are multiple ways of finding large primes. One of them is by picking random numbers and checking their primality. This method is used to generate the large primes needed for RSA cryptosystems. A random 2048-bit number is chosen. It's first bit is set to one to ensure a large enough number and it's last bit is set to one to make it odd. Then the primality of the number is checked.

The Prime Number Theorem [Weisstein, 2021] states that there are approximately $n \ln(n)$ primes $p \leq n$. This gives that the probability of choosing a random number below some integer n and finding a prime is equal to $1/\ln(n)$, since there are n possible number to choose from and there are $n \ln(n)$ primes.

For RSA cryptosystems, numbers below 2^{2084} are chosen

However, for finding primes much larger, this method is too slow. For our use, we designed a program that would loop over all mersenne numbers $M_p = 2^p - 1$ with p prime and then check it's primality using the Lucas-Lehmer primality test.

References

[Bruce, 1993] Bruce, J. (1993). A really trivial proof of the lucas-lehmer test. https://fermatslibrary.com/s/a-really-trivial-proof-of-the-lucas-lehmer-test. Accessed on 22-10-2021.

[Weisstein, 2021] Weisstein, E. W. (2021). Prime number theorem. https://mathworld.wolfram.com/PrimeNumberTheorem.html. Accessed on 26-10-2021.