Methods of testing for prime numbers and showing that they are prime

Student

August 20, 2024

Abstract

This essay is based on the 3^{rd} and 4^{th} chapters of the book "Prime Numbers a Computational Perspective" by Richard Crandall and Carl Pomerance [2]. Unless stated otherwise, definitions, theorems and proofs of theorems in sections 2 to 6 are based on results described in these chapters.

Contents

1 Introduction

Prime numbers are a very important area of mathematics. In cryptography, prime numbers are used to secure bank transactions as well as RSA encryptions by multiplying two very large prime numbers together. Examples like this show that being able to determine whether a number is prime or not is extremely useful. In this essay I will consider some methods for identifying possible prime numbers and later ways to show that a number is prime.

Our first task is to check whether there is a finite number of prime numbers.

Lemma 1.1. *there are infinitely many prime numbers.*

Proof. Assume we have N prime numbers. Consider

$$S = \prod_{i=1}^{N} P_i + 1 : \text{P is prime}$$

We now note that for each $i \in [1, N]$, P_i does not divide S. We can therefore conclude that S is prime. □

Given there will be no largest prime number, we now consider various tools to identify primes

2 Some useful results

In our analysis of prime number testing we will encounter several algorithms. With these algorithms, the main downside to them will be the time required to complete them. Thus when we give an overview of the advantages and disadvantages of these, we will need to consider the length of time it would take a computer to implement them.

Definition 2.1 (Big-O notation)**.** If we have a fixed $C > 0$ and two funtions f and g such that

$$|f(x| \leq C\,|g(x))|$$

for every $x \in \mathbb{N}$ then f is called the *big-O* of g

Definition 2.2. The *Prime counting function*, denoted $\pi(x)$, is defined as the number of prime numbers less than or equal to x.

From this, we obtain a very simple result

Corollary. *It is possible to describe* $\pi(x) = O(x)$.

Proof. This follows from the fact that the number of primes less than or equal to x is bounded above by x. □

Definition 2.3 (little-o notation)**.** Suppose that $f(x)$ and $g(x)$ are functions and

$$\lim x_{\to\infty} f(x)/g(x) = 0$$

. Then we have that $f(x) = o(g(x))$

In order to consider the sieve of Eratosthenes, we need to put an approximation to how many primes we can expect to be less than or equal to N where N becomes large.

Definition 2.4. A function f is *asymptotic* to g if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

. We denote this by $f(x) \sim g(x)$

Theorem 2.1 (Prime Number Theorem)**.** *The prime counting function $\pi(x)$ is asymptotic to $\frac{x}{\log(x)}$. In other terms, for large values to x, $\pi(x) \approx \frac{x}{\log(x)}$.*

The proof of this theorem requires the knowledge that $\zeta(s)$ has no zeros with $\Re(s) = 1$ where $\zeta(s)$ is the Riemann Zeta function, and $\mathfrak{R}(s)$ is the real part of the complex plane, as explained in "Newman's short proof of the prime number theorem", found in [6]. As a result, a full proof of this result will not be given here, but will help us estimate the efficiency of the Sieve of Eratosthenes.

3 Sieve of Eratosthenes

The simplest test for primality testing is an algorithm known as the *Sieve of Eratosthenes*. This is an algorithm which takes an array of $N-1$ numbers and begins with a 1 representing each of the numbers, usually beginning with 2 and ending with N. We describe the most basic algorithm below.

Algorithm 3.1 (Sieve of Eratosthenes)**.** Step 1: consider the first number which is given a 1 in the array and label it p. Step 2: Go to the entry p^2 and change its label to a 0 if it isn't already. (This minor improvement is suggested in the article "The Genuine Sieve of Eratosthenes" [4]. Step 3: From p^2, pass over all other multiples of p and label them 0. If the value of the multiple exceeds N, move to step 4. Step 4: Consider the smallest remaining value n which is assigned a 1. If $n^2 > N$, the algorithm terminates. Otherwise, return to Step 1

Remark. The Sieve of Eratosthenes can also be adapted to have an arbitrary starting point L. For an interval (L, R) with L and R even, find a value B which divides $R-L$. We also require that $L > \lceil\sqrt{R}\rceil$. Denote $L > \lceil\sqrt{R}\rceil = P$ and assume it possible to "make a table of of the $\pi(P)$ primes $p_k \leq P$".[2, p. 122] Begin at the first entry and let $q_k = (-\frac{1}{2}(L+1+p_k)) \bmod p_k$. Then

for each $j \in [0, B-1]$, where $k \in [2, \pi(P)]$, if $j < B$, then, starting with $j = q_k$, set $j = j + p_k$ and $b_j = 0$. Reset $q_k = (q_k - B) \bmod p_k$ and repeat the algorithm

We now present 2 examples of how the Sieve of Eratosthenes would work in practice.

Example 3.1. We perform the Sieve of Eratosthenes on the array of numbers less than or equal to 101.

Initialising the array: we begin by giving a 10×10 matrix with each entry being 1

$$A_0 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

which represents the values in

$$A = \begin{pmatrix} 2 & 3 & \cdots & 11 \\ 12 & 13 & \cdots & 21 \\ \vdots & \vdots & \ddots & \vdots \\ 92 & 93 & \cdots & 101 \end{pmatrix}$$

The first value in this matrix represents 2, so within our matrix A_n (here n represents the number of iterations of the Sieve that have been completed), we continue to represent 2 with a 1 and declare it prime. Starting with $2^2 = 4$, we change the value to a 0. thus we have

$$A_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & \cdots & 1 \\ 0 & 1 & 0 & 1 & 0 & \cdots & 1 \\ 0 & 1 & 0 & 1 & 0 & \cdots & 1 \\ 0 & 1 & 0 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & 0 & 1 & 0 & \cdots & 1 \end{pmatrix}$$

Now the first remaining 1 that has not been used represents 3, so beginning with the 9 value, all multiples of 3 are changed to 0, thus

$$A_2 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

By the end of 4^{th} iteration our matrix becomes

$$A_4 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

We now see that the next 1 value is 11 which is greater than $\sqrt{101}$, so we can terminate the algorithm and declare that our primes between 2 and 101 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 and 101, as suggested by our final array.

3.1 Disadvantages of the Sieve of Eratosthenes

The Sieve of Eratosthenes is a very accurate way of determining the primality of a number. If the final output of the Sieve of Eratosthenes gives a 1, the value in question is definitely prime. The drawback is that the algorithm is so slow that where N becomes large, the length of the array becomes so large that it will take more than a computer's lifetime to execute. The usual implementation of the Sieve of Eratosthenes requires

$$\sum_{i=1}^{\pi(\sqrt{N})} \frac{N}{p_i}$$

considerations, which we will approximate by the prime number theorem. Based on the work in Melissa O'Neill's article [4] we have that

$$\begin{aligned}
\sum_{i=1}^{\pi(\sqrt{N})} \frac{N}{p_i} &\approx \sum_{i=1}^{\frac{2\sqrt{N}}{\log(N)}} \frac{N}{p_i} \\
&\approx \frac{N}{2} + N \sum_{i=2}^{\pi(\sqrt{N})} \frac{N}{p_i} \\
&\approx \frac{N}{2} + N \sum_{i=1}^{\frac{2\sqrt{N}}{\log(N)}} \frac{1}{i\log(i)} \\
&\approx \frac{N}{2} + N \int_{2}^{\frac{2\sqrt{N}}{\log(N)}} \frac{1}{i\log(i)} di \\
&\approx \frac{N}{2} + N \int_{\log(2)}^{\log(\frac{2\sqrt{N}}{\log(N)})} u^{-1} du \\
&\approx N\log(\log(N)) + O(N)
\end{aligned}$$

Where we have approximated $\pi(\sqrt{N})$ using the prime number theorem in both the upper limit and the sum, and we have used the substitution $u = \log(i)$ for the integral. The first issue with implementing the Sieve of Eratosthenes is the amount of computer space it occupies. As the number of values to be tested increases, the size of the full array of numbers to use becomes too large. An obvious idea for a solution would be to reduce the size of this array and still check for prime numbers in this range. However, the consequence of this is that the time for the Sieve to complete begins to get large. For an array of length M with primes up to $\sqrt{N}$ the time the sieve takes is proportional to

$$M\log(\log(N)) + \pi(\sqrt{N}) + O(N)$$

, of which the term $\pi(\sqrt{N}$ will increase extremely quickly. We thus need a more efficient method to determine prime numbers. However, it will turn out that these are not entirely accurate, so they will work alongside the Sieve of Eratosthenes.

4 Fermat pseudoprimes and Carmichael numbers

4.1 Fermat's Little Theorem

Before we introduce Fermat's little theorem, we will use the binomial theorem to introduce a lemma. The proof shown is very standard and can be found in many places, one of which is in the third chapter of Robert E Bishop's article "on Fermat's Little Theorem" [1]

Lemma 4.1. *For integers a and b and a prime number p, we have that*

$$(a+b)^p \equiv a^p + b^p \mod p$$

Proof. We will use the formula for binomial coefficients to show that each of these will divide p. By the binomial theorem, we have that the k^th coefficient of $(a+b)^p$ is given by

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

. Now for any $0 < k < p$, neither $k!$ nor $(p-k)!$ will be divisible by p as they contain values strictly less than p and p cannot be factorised. Given $p!$ is divisible by p, we know that $\binom{p}{k}$ is divisible by p. □

Theorem 4.2 (Fermat's Little Theorem)**.** *Suppose p is a prime number. Then for any integer base a, we have that*

$$a^p \equiv a \mod p$$

Proof. We will prove the result by (weak) induction on a. If $a = 1$, the result is trivial given that $1^n = 1$ for any value of n. Now suppose for our induction hypothesis that

$$a^{p-1} \equiv 1 \mod p$$

or, equivalently

$$a^p \equiv a \mod p$$

(as long as a and p are coprime) which has been obtained by multiplying through by a. Now using the above lemma,

$$(a+1)^p \equiv a^p + 1^p \mod p$$

. As $a^p \equiv a \mod p$ by assumption, $(a+1) \equiv a+1 \mod p$, so we conclude our proof by induction. □

Fermat's Little Theorem would give an extremely powerful test to see whether a number is prime if the converse was also true. It seems that if, for any base (we may want to check this by induction), our output $\mod p$ is the base, then p is prime. However, it turns out that the converse to Fermat's Little Theorem is not true. We will see some examples below of numbers which satisfy the conditions for Fermat's Little Theorem but are not prime.

4.2 Fermat pseudoprimes

We will begin this section with a definition.

Definition 4.1. A *Fermat pseudoprime base a* is a value n satisfying $a^n \equiv a \mod n$ but is not a prime value.

We now present an example of a Fermat pseudoprime, before looking at two useful results.

Example 4.1. we have $3^{90} \mod 91 \equiv (3^6)^{15} \mod 91$. Now $3^6 = 729$ is one more than $728 = 91 \times 8$, so $3^6 \equiv 1 \mod 91$, thus,$3^{91} \equiv 3 \mod 91$ so 91 is a pseudoprime base 3 (along with any other composite number 1 greater than a multiple of 6).

There is, however, hope that as our values of n increase, the likelihood of n satisfying Fermat's Little Theorem will be a pseudoprime is going to reduce. This turns out to be the case.

Theorem 4.3. *For each fixed integer $a \geq 2$, the number of pseudoprimes less than or equal to x is $o(\pi(x))$. Specifically,*

$$f(x) < xe^{-\frac{1}{3}\log(x)^{\frac{1}{4}}}$$

.

Proof. We will outline the proof from Paul Erdos' article "On Almost Primes" [3]. Let $g(n)$ be the least positive exponent satisfying $2^{g(n)} \mod n$. We split our values of g into 2 cases. For our first case, consider when $g \leq e^{(\log(x))\cdot 5} = H$. Consider $P = \prod_{r=1}^{H}(2^r - 1)$. Given that for each $g(n)$, $2^{g(n)}$ divides n, they are factors of P. The next step is to split this class of values into two subclasses, Γ_1 and Γ_2. First, consider those which have less than $W = \frac{1}{10}\log(x)^0.5$ distinct prime factors. Using the fact that there will be a value $m \leq x$ in this class with 2^α dividing m, we can state that Γ_1 has less than $Wk^W(\frac{\log(x)}{\log(2)})^W$ elements, where k is the number of prime factors of P. For x sufficiently large, this is less than $x^{\frac{1}{4}}$. For Γ_2, let $d(m)$ be the number of divisors of m and $v(m)$ be the number of distinct prime factors of m. □

This result is useful because it means the probability that a large number that satisfies Fermat's Little Theorem is prime will tend to 1 as n becomes large. There are, however, two potential issues. Firstly, it turns out that as well as having infinitely many primes, there are also infinitely many Fermat pseudoprimes for each base. It is interesting to note that this fact is a direct consequence of the infinity of prime numbers

Theorem 4.4. *For each base a, there are infinitely many Fermat pseudoprimes.*

Proof. Let $p > 2$ be a prime number, and a a base such that $p \nmid a^2 - 1$. Consider

$$n = \frac{a^{2p} - 1}{a^2 - 1}$$

. By the difference of two squares formula, we can write n as

$$\frac{(a^p - 1)(a^p + 1)}{(a-1)(a+1)} = \frac{a^p - 1}{a-1}\frac{a^p + 1}{a+1}$$

. By Fermat's Little Theorem, we know that both of these fraction terms are integers, so n is composite. By squaring the statement of Fermat's Little Theorem, we obtain that

$$a^{2p} \equiv a^2 \mod p$$

. Given that p does not divide $a^2 - 1$, and that $n - 1 = \frac{a^{2p} - a^2}{a^2 - 1}$, p divides $n - 1$. Given there are infinitely many primes that do not divide a fixed $a^2 - 1$, there are infinitely many pseudoprimes base a. □

4.3 Carmichael numbers

We have seen above that for a base a, a^{n-1} being divisible by n does not guarantee primality. What, however, can we say about n if a^{n-1} is divisible by n for *every* choice of a. The answer, perhaps surprisingly, is nothing.

Definition 4.2. A *Carmichael number* is a value n for which Fermat's Little Theorem holds for *any choice* of a, yet n is *composite*.

At first glance, it seems highly unlikely that such a value will exist. However, it turns out that the composite number $561 = 3 \times 11 \times 17$ satisfies $a^5 61 \equiv a \mod 561$. We now set up a theoretical criterion for a number being Carmichael.

Theorem 4.5 (Korselt criterion)**.** *An integer n is a Carmichael number if and only if n is positive, squarefree and if $p \mid n$, $(p-1) \mid (n-1)$*

Before we give a proof, we will first introduce the notion of a primitive root

Definition 4.3. A *primitive root modulo n* is an integer a such that for any c coprime to n, there is some integer x such that $c = a^x \mod n$

Proof. We will begin by proving the forward direction. Let p be a prime factor of n. From the fact that n is a Carmichael number, $p^n \equiv p \mod n$, so $p^n - p \equiv 0 \mod n$. Writing $n = xp$ for integer x, we have that $xp \mid (p^n - p)$, and therefore $x \mid (p^{n-1} - 1)$. However, as $p \nmid (p^{n-1} - 1)$, p cannot be a factor of x and therefore $p^2 \nmid n$, so n is squarefree. Let a be a primitive root modulo p. Therefore $a^n \equiv a \mod n$, so $a^n \equiv a \mod p$ (as $p \mid n$). Thus $a^{n-1} \equiv 1$

mod p, however, given that a is a primitive root modulo p, $a \mod p$ has order $p-1$, so $p-1$ divides $n-1$.

For the converse, assume that for each $p \mid n$, $(p-1) \mid (n-1)$, as well as n being squarefree and composite. For these reasons, we note that it suffices to show that $a^n \equiv a \mod p$ for every integer a and all $p \mid n$. Note that $a^{n-1} \equiv 1 \mod p$ as $(p-1) \mid (n-1)$ and by Fermat's Little Theorem. This means that $a^n \equiv a \mod p$, which holds for all values of a. □

Therefore, we can easily conclude that 561 is a Carmichael number, given 2, 10 and 16 all divide 560.

5 Smooth Numbers

Suppose that for a possible prime number n, we could put an upper bound to the values of its factors. This could then potentially make the process of finding prime numbers a little quicker. If we know that there is no prime factor exceeding a known prime number, it is logical to assume that this will help speed up an algorithm for finding prime numbers. As it turns out, as we will discuss in section 5.3, smooth numbers can help convert an algorithm's run time to almost polynomial. We will start by defining the notion of a smooth number below.

5.1 Definition

Definition 5.1. A *y-Smooth number* is defined as a number x such that x has no prime factors greater than y.

It is important to note that the definition of a smooth number is dependent on having a useful and known prime valued number to use to compare to, so for large values of x and y this may become difficult. We present some examples below.

5.2 Examples

Example 5.1. The number $985 = 5 \times 197$ can be described as 199 smooth, given both 5 and 197 are less than 199. However, 985 is not 193 smooth, as it has a factor greater than 193.

Example 5.2. The number $99777 = 3 \times 79 \times 421$ is 443 smooth given all of its prime numbers lie below 443. It is, however, not 389 smooth as that value is less than 421.

5.3 Uses of smooth numbers in prime testing algorithms

The main reason for considering smooth numbers for prime number testing is how they speed the process of finding these. We begin by assuming that

for a prime number p, $p-1$ is y-smooth for some odd number y, with 2 the only other prime factor. It then turns out that there will be more than $x^{\frac{2}{7}}$ Carmichael numbers up to x, using a result on y^c (see [5][p420]). Another helpful improvement of considering smooth numbers is to reduce primality proving algorithms to "'almost' polynomial time" , as suggested in the Pomerance article "The role of smooth numbers in number theoretic algorithms" [5]. We move on to discuss two of these tests in our next section.

6 Tests to prove primality

We conclude this essay with some ways of showing that a possible prime candidate is indeed prime.

6.1 Lucas Theorem

Thankfully for us, in order to show use Fermat's Little Theorem to show a number *is* prime, we only require one additional condition. Before this, we need to introduce a new function.

Definition 6.1. *Euler's totient function* $\varphi(n)$ is defined as the order the group of units in $\mathbb{Z}/n\mathbb{Z}$.

We will use this to prove the following result,

Theorem 6.1 (Lucas theorem)**.** *Let a and n be integers, with $n > 1$. If we have that $a^{n-1} \equiv 1 \mod n$* and *that the order of $a \mod n$ is $n-1$, then we can conclude n is prime. Equivalently, for a prime q such that $q \mid (n-1)$,$a^{\frac{n-1}{q}} \equiv r \mod n$, where $r < n$ and $r \neq 1$*

before we prove this result, we remind ourselves of Euler's theorem, which states that $a^{\varphi(m)} \equiv 1 \mod m$. From Euler's theorem and Fermat's Little Theorem, we can immediately see that when p is prime, $\varphi(p) = p-1$. We now give the proof of the Lucas theorem

Proof. Assume that n is composite for a contradiction. We know that the order of a has to divide $\varphi(n)$ from Euler's theorem, so $n-1 \leq \varphi(n)$. If n is composite, we have $n-1 < \varphi(n)$. Assume p is a prime factor of the composite number n. We then know that $p, n \leq n$ and these are not coprime to n, so the order of n will be less than or equal to $n-2$. This contradicts that $n-1 \leq \varphi(n)$, so we conclude that n is prime. □

This result gives us a powerful test as to whether a number is prime. We now consider a test for Fermat numbers, and we begin by introducing them.

Definition 6.2. A *Fermat number* is a number of the form $2^{2^k}+1$, with $k \in \mathbb{Z}$. If this is prime, it is called a *Fermat prime*. We denote this as F_k.

6.2 Pepin's test

Before giving the Pepin test, we need to introduce some terminology.

Definition 6.3. Let a and m be coprime integers. We say that a is a *quadratic residue* $\mod m$ if and only if the congruence

$$x^2 \equiv a \mod m$$

has a solution. It is said to be *non-quadratic residue* if not

Definition 6.4. Let $p > 2$ be a prime number and The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ if } a = 0 \mod p \\ 1 \text{ if } a \text{ is a qudratic residue} \mod p \\ -1 \text{ if } a \text{ is not a quadratic residue} \mod p \end{cases}$$

We also bring the following result about the Legendre symbol

Proposition 6.2. *for m, n coprime,*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$$

We will use this terminology to help us prove the following result. Before this we need to introduce Euler's criterion.

Theorem 6.3 (Euler's criterion)**.** *Where p is a prime number,* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$

With these results set up, we now introduce the Pepin test.

Theorem 6.4 (Pepin test)**.** *For $k \geq 1$, F_k is prime if and only if*

$$3^{\frac{F_k-1}{2}} \equiv -1 \mod F_k$$

Proof. We begin by assuming the the congruence. Using the Lucas theorem with $a = 3$ and $q = 2$, we conclude that F_k is prime. Conversely, assume F_k is prime. Given that 2^k is even, it turns out that $2^{2^k} - 1$ is divisible by 3 (this is easily checked by induction). Thus $F_k \equiv 2 \mod 3$ and $F_k \equiv 1 \mod 4$, so $\left(\frac{3}{F_k}\right) = \left(\frac{F_k}{3}\right) = -1$, as $\frac{F_k-1}{2}$ is even. Thus by Euler's criterion, the congruence holds □

We now show an example of how prime candidates perform in these 2 tests.

Example 6.1. We have already seen that the Carmichael number 561 is not a prime. To prove this without factorisation, consider $560 = 2^4 \times 7 \times 5$ and consider $2^{(\frac{560}{7}=80)} \equiv 1 \mod 561$, so 561 cannot be prime.

Example 6.2. Consider F_3. We will evaluate $3^{\frac{F_3-1}{2}} \mod F_3$. It turns out that $3^{128} \equiv -1 \mod 257$, so F_3 is prime.

References

[1] Robert E Bishop. On fermat's little theorem. *preprint*, 2008.

[2] Richard Crandall and Carl Pomerance. *Prime Numbers a Computational Perspective*. Springer, 2nd edition, 2005.

[3] Paul Erdos. On almost primes. *American Mathematical Monthly*, pages 404–407, 1950.

[4] Melissa E O'Neill. The Genuine Sieve of Eratosthenes. *Journal of Functional Programming*, 19(1):95–106, 2009.

[5] Carl Pomerance. The role of smooth numbers in number theoretic algorithms. In *Proceedings of the International Congress of Mathematicians*, pages 411–422. Springer, 1995.

[6] Don Zagier. Newman's short proof of the prime number theorem. *The American mathematical monthly*, 104(8):705–708, 1997.