PRIMALITY TESTING

Erick Calderon   Christian Coirin   Hasti Mehta   Savannah Nichols
University of Illinois at Chicago

MSCS Undergraduate
Research Laboratory

UIC

About this project

This project was supervised by Evangelos Kobotis. There were weekly zoom meetings in which we went over theoretical points, set goals and discussed our results.

Motivation

The general purpose of this project was to serve as an introduction to programming as well as the theory of prime numbers. Our main goal was to identify large prime numbers and to go over the different means of testing primality.

Methodology

During our meetings everyone was engaged, bringing new ideas, discussing their successes and failures with the assignments of the previous week, volunteering for the new tasks or giving suggestions for different directions. The role of this presentation is to summarize some of the work that we did. In many cases we took code segments from the web but overall the code and results that we generated were our own work. We made every effort to give credit to our outside sources.

Starting with an ancient algorithm

Exploring the properties of the set of prime numbers is one of the most fascinating and difficult tasks in mathematics. We began by looking over an ancient algorithm that theoretically produces all prime numbers.

This is the Eratosthenes sieve and it is based upon the fact that every composite natural number is divisible by a prime number that does not exceed its square. Indeed if n is composite, then it can be written as ab where a and b are natural numbers greater than 1. If $a \geq b$, then $b^2 \leq n$ and if p is any prime number dividing b then $p^2 \leq n$ or $p \leq \sqrt{n}$.

This simple property has the following implication. If we start with the set:

$$\{1, 2, 3, \ldots, k^2\}$$

and we strike out 1 and all the numbers that are divisible by primes not exceeding k, then the numbers that are left behind are precisely the primes that are between k and k^2. In other words, if we know the primes that are less than k then we can easily find the primes that are less than k^2. More concretely, if we begin with the primes $2, 3, 5, 7$ that are precisely the primes that do not exceed 10, then we can easily find the primes that do not exceed 100. Once we can accomplish that, then we can easily find the primes not exceeding 10,000 and so on. We did find 5,761,455 primes less than 10^8.

Fermat's Theorem

Fermat's theorem states if p is prime then, for any integer a, the number $a^p - a$ is an integer multiple of p.
This can also be stated as:

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

The above symbol is a congruency symbol. Two numbers are congruent if, when divided by the same number, they have the same remainder.
To use this test we first pick an arbitrary integer a. We then raise a to the $n-1$ power and divide by n. If the remainder is 1, then n is prime.
It is important to note this test is probabilistic, meaning, that not all numbers found using this test are prime. Primes found with this method require additional testing to be considered prime. While this test is not deterministic, the simplicity of it allows for fast run times, making it a valuable method of sieving out composite numbers.

The Prime Number Theorem

The Prime Number Theorem was conjectured by Carl Friedrich Gauss and Jean-Marie Legendre. In modern terms, it states that if we set $\pi(x) = \#\{p \;\text{ prime} : p \leq x\}$ then

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$$

For 10^8 we get to get 5,761,455 prime numbers and the Prime Number Theorem predicts 5,428,681 primes.

For $10^8 + 10^6$, we get 5815663 prime numbers while the Prime Number Theorem predicts 5480007 primes

Trivial and Accessible Range

Our first task was to produce a list of prime numbers under 10^8. We were able to produce this list using a classical method, the eratosthenes sieve. We have denoted these numbers under 10^8 as the trivial range because the primes in this range can be quickly identified using the before mentioned eratosthenes sieve. We consider numbers from 10^8 to 10^{16} to be the accessible range because these primes can be found in a reasonable run time by eliminating the multiples of the primes found in the trivial range.

Numerical results in the accessible range

Let's begin by taking a look at the interval $[10^{10}, 10^{10} + 10^6]$. The prime number theorem projects that there are going to be 43,429 primes in this range. We begin by sieving out all the multiples of primes in the trivial range (recall that the trivial range consists of all numbers up to 10^8). Then we find 43,427 primes: a number which is suprisingly close to what is predicted by the Prime Number Theorem. If we repeat this in the interval $[10^{11}, 10^{11} + 10^6]$ then we find 39,434 primes compared to 39,484 primes that are predicted by the Prime Number Theorem.

Prime Numbers beyond the accessible range

We combine everything that we've learned in our research in order to be able to find prime numbers beyond the accessible range. (10^{16}).

We start off similar to how we would when we find primes within the accessible range. We sieve out all composite numbers within the trivial range, leaving only prime numbers that are $< 10^8$. We then select a smaller range from beyond the accessible range and sieve out any multiples of the trivial primes. This is the same as we did when we selected a smaller range from within the accessible range. The difference here is that any numbers from within this smaller range, that were not sieved out by the trivial primes, can not be considered prime just yet. This is because, as explained by the Eratosthenes Sieve, the trivial primes will only be able to perfectly sieve out composite numbers up to $(10^8)^2$, which is how we got 10^{16} as the end of our accessible range in the first place. So there could be prime numbers that are not multiples of any trivial primes at this point.

These numbers found beyond the accessible range, that were not sieved out, are considered *probable primes*. We now implement the other tests we've discussed. We first use the Miller-Rabin test. We choose one of the probable primes, n, and perform the Miller-Rabin test. If it fails then n is determined to be composite. If it passes, then n is considered a strong probable prime.

We then take this probable prime, n, and perform the AKS test, step by step. We perform step 1, to determine whether n is a perfect power. If n is a perfect power, it is determined to be composite, if not, move on to step 2. We perform step 2 to find the smallest integer, r, such that the multiplicative order of n modulo $r > (\log_2 n)^2$. We skip steps 3 and 4 because as explained earlier, they are rather useless for our research purposes. We move on to step 5 and if n passes this step, n can now be determined to be a prime number.

Examples of prime numbers we have found using this method:

- 13,666,666,666,666,613
- 19,019,684,767,739,993
- 22,222,223,333,355,757
- 44,444,446,666,688,899
- 99,999,999,999,899,999
- 1,000,000,000,000,000,003

Miller-Rabin test

The **Miller-Rabin test** is also probabilistic and it is based on the following process. We have a number n and we consider a number a which is coprime to n. We then write $n - 1 = 2^s m$, where m is an odd number. We then test to see if the numbers

$$a^m, a^{2m}, \ldots, a^{2^s m}$$

are all equal to 1 with the possible exception of the first one that could be -1. If this is the case, then the test is passed by n and it has a strong probability to be a prime number.

The Fibonacci test

The Fibonacci test is conjecturally deterministic, meaning, while there is no formal proof that the numbers found with this method are prime, it has never produced a composite number. Therefore we can assume with high probability that the numbers found using this method are prime. The test states that if n is prime then:

$$F_{n-(\frac{5}{n})} \equiv 0 \pmod{n}$$

First we compute $(\frac{5}{n})$. This is done by computing $n \pmod{5}$. If $n \pmod{5} = 1$, then the function outputs 1. If $n \pmod{5} = 0$ then the number is composite. If $n \pmod{5} \geq 2$ then the function outputs 0.
Next we compute $F_{n-(\frac{5}{n})}$. In order to do this we must generate the sequence of fibonacci numbers up to the $n - (\frac{5}{n})$ term and take this number to be $F_{n-(\frac{5}{n})}$.
Finally we divide $F_{n-(\frac{5}{n})}$ by n. If $F_{n-(\frac{5}{n})}$ is divisible by n, then n is prime.

The AKS Primality test

The AKS test, unlike the Miller-Rabin test, is deterministic. However, it is very complex and lengthy. Because of this, the AKS test is the last step we take for finding primes that are beyond the accessible range. It consists of a total of 5 steps.

Step One: Check if probable prime, n is a perfect power. In other words, is $n = a^b$? If this is true, then n is determined to be composite, otherwise, n remains a probable prime and we move to step two.

Step Two: Find the smallest integer, r, such that $ord_r(n) > (\log_2(n))^2$. Here $ord_r(n)$ is the *multiplicative order* of n modulo r. The multiplicative order of n modulo r is the smallest positive integer, k, such that $n^k \cong 1(\mod r)$. This integer, r that we find in this step will be used in the next steps

Step Three: For all a such that $2 \leq a \leq min(r, n-1)$ check that a does not divide n. If a number a is found to divide n, then n is composite. Otherwise, move to step four.

Step Four: Check if $n \leq r$. Just like step three, this step is trivially correct. r is expected to be significantly less than n, so we do not expect any of the large probable primes we deal with to fail this test

Step Five: For, $a = 1$ to $\lfloor \sqrt{\phi(r)} \log 2(n) \rfloor$, check if $(X + a)^n \neq X^n + a (\mathrm{mod} X^r - 1, n)$. Here, $\phi(r)$ is known as Euler's theoretic function, it is the total number of integers, which are less than r, that are coprime (have a greatest common divisor equal to 1) to r. Floor simply means to round down to the nearest integer. X is simply a variable, making the above expression a polynomial. If the above expression is found to be true, then n is determined to be composite. Otherwise, we can finally determine that n is indeed prime.