NUMERICAL ADVENTURES WITH PRIME NUMBERS

Subash Bhusal   Eddie Federmeyer   Jamie Hayes   Vivek Ily   Nero Partida   Erik Raaum   Nicholas Ruffolo
University of Illinois at Chicago
MSCS Undergraduate Research Laboratory

Supervised by

Evangelos Kobotis

Motivation

The general purpose of this project was to explore the theory of prime numbers through a series of numerical experiments. Our main goals have been to study general and special properties of prime numbers and to understand the difficulties and limitations that one comes across while trying to translate the theory into actual usable information.

Elementary approach and choice of range

Our first task was to produce a list of prime numbers. To this end we came up with all prime numbers that do not exceed 10^8. This can be achieved by using quite classical means in a very small amount of time. This allowed us to start a further programming task by generating the primes in this range and then manipulating them as desired. In this way we were able to look for special kinds of primes, analyze their distribution and in general get acquainted with the speed that it takes to solve numerical problems like this in the range that we ended up referring to as the *trivial range*.

Beyond the trivial range

Our intention was to move outside the trivial range and explore things beyond its confines. The classical problem of finding large primes interested throughout the duration of this project. We did not have the ambition to find the next largest prime - that would have been pointless. We wanted however to find really large prime numbers, possibly prime numbers that have not been identified up to this point.

Additional exploration

Simultaneously we sought to examine interesting and possibly more advanced parts of the theory of prime numbers. We looked at connections between the Prime Number Theorem and numerical applications. We engaged in a graphical exploration of the Ulam spiral. We looked at conjectural primality tests. We conducted numerical tests linked to the Dirichlet's theorem on primes in arithmetic progressions.

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.

Special types and patterns of prime numbers

Two primes are called **twin primes** if they differ by 2. In other words twin primes come in pairs. However, we can call a prime twin if it belongs to a pair of twin primes.

An odd prime p is called a **Germain prime** if $2p+1$ is also a prime number. We found more than 423,140 Germain primes less than 10^8.

A prime number is called **palindromic** if (in base 10) its representation is a palindrome. For example 101 is a palindromic prime. We found about 6,000 palindromic primes less than 10^8.

A prime number p is called **regular** if its the class number of the number field $\mathbb{Q}(\zeta_p)$ is not divisible by p. It turns out that a number p is prime if and only if it does not divide the numerator of any of the Bernoulli numbers $B_2, B_4, \ldots B_{p-3}$. Finding the Bernoulli numbers was one of the most tedious tasks that we performed.

A **Mersenne prime** is prime of the form $2^p - 1$ where p is a prime number. The largest prime numbers that have ever been found are Mersenne primes. It was no big surprise that we found just 7 Mersenne primes in our range, the largest being 524,287.

A **permutable prime** is a prime number that remains prime no matter how its digits are permuted. For example 13 is a permutable prime. There was a very limited amount of permutable primes in the range that we studied - none of them with more than 3 digits.

Another interesting topic is **arithmetic progressions of prime numbers**. The Green-Tao theorem suggests that there exist arbitrarily long arithmetic progressions among prime numbers. We would like to know how much we can say about the trivial range. We did find numerous progressions with six terms in our range.

We also looked at **gaps between prime numbers**. The largest gap that we ended up finding in our range was 220.

Dirichlet's theorem on primes in arithmetic progressions

Two integer numbers a and b are called coprime if and only if their only common divisor is the number 1. If a and b are natural coprime numbers, then according to Dirichlet's theorem, there exist infinitely many prime numbers of the form $an+b$. In fact it can be shown that for a given number a, the amounts of primes that correspond to the different remainders of division by a are uniformly distributed.

We looked at prime numbers of the form $100n + a$ where a can be any number between 1 and 100 which is coprime to 100. There are actually 40 such numbers. We then looked at the primes less than 10^8 and classified them according to their remainder upon division by 100. It turned out that the proportions were almost perfectly distributed as projected by Dirichlet's theorem and its extensions. In fact the average proportion ended up being 0.025000000000000005!

The Prime Number Theorem

The Prime Number Theorem states that the amount of prime numbers that does not exceed x is approximately $x/\log x$. One of the functions used in the process of proving the PNT is Chebyshev's theta function:

$$\vartheta(x) = \sum_{p \leq x} \log p$$

In fact the Prime Number Theorem itself is equivalent to the statement that:

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

It is also quite interesting that it has been proven that $\vartheta(x) - x$ changes sign infinitely many times. We wanted to explore this property by finding the sign of this expression in the trivial range.

It turns out that $\vartheta(x) - x$ never changes sign in this range. In fact, one has to go to astronomically large numbers in order to observe the first change in sign.

Primality testing

Finding large prime numbers is one of the main goals in the theory of prime numbers. Here we apply a simple-minded search based on several theoretical results that we mention below. There are several primality tests. Some of them are probabilistic. Other are deterministic. Probabilistic primality tests identify numbers that have a strong probability of being prime. Deterministic tests, prove, when certain conditions are satisfied, that a given number is prime.

For some of this tests, it is useful to know Fermat's little theorem according to which if p is prime then for any integer a not divisible by p, we have:

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

This means that if we have a number n for which the congruence:

Primality testing (continued)

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

is wrong for a given a that is coprime to n, then it cannot be a prime number. On the other hand, if this is correct for a given a which is coprime to n, then this may make us hope (but certainly not decide) that n is prime. In fact this is the content of the **Fermat Primality Test**. One chooses a number a less than n and tests the equality $a^{n-1} \equiv 1 \mod n$. If it is true then we think of n as having some probability of being prime.

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.

It is conjectured that the following test is deterministic. If n is natural number satisfying:

- $2^{n-1} \equiv 1 \mod n$
- $F_{n+1} \equiv 0 \mod n$

then n is a prime number. Here F_{n+1} is the $n+1$-th term of the Fibonacci sequence defined by $F_0 = F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$.

We looked for big prime numbers using the following elementary method. We chose a segment of natural numbers beyond the trivial range - say of length 10,000. We sieved out all multiples of prime numbers that do not exceed 10,000 and then we applied a probabilistic test like the Miller-Rabin test to the remaining numbers. Thus we got numbers that have a strong probability of being primes. To these we applied the Fibonacci primality test, which is conjectured to be deterministic.

Prime numbers and graphics

Primes are in general very irregularly distributed. However there are some very striking attempts to visualize prime numbers within the natural numbers. One such visualization attempt is through the Ulam spiral.

Here is a visualization based on the Ulam spiral cycle of ideas. The general prime numbers are depicted in blue and the Germain primes in pink.