THE QUEST FOR PRIME NUMBERS

Mohammed Ahmed Krishn Patel Sedrik Punzalan Parineet Sond
University of Illinois at Chicago

MSCS Undergraduate Research Laboratory

The Eratosthenes Sieve

For our first attempt to understand prime numbers, we need the fact that every composite number n has a prime divisor that does not exceed $\sqrt{n}$. This allows us to consider an ancient method for finding primes, known as the Eratosthenes sieve. Its idea is pretty simple. Start with an initial segment of natural numbers up to n and suppose that all primes that do not exceed $\sqrt{n}$ are known. Then delete all multiples of these primes up to n (but not the prime themselves) along with the number 1, and what is left behind are all the primes that do not exceed n. This is shown below for $n = 100$:

It is clear that this can be used over and over in order to find more and more prime numbers. The Eratosthenes sieve has many practical limitations and in our case we used it in order to determine all primes that do not exceed 10^8. We named this range the trivial range.

The Fermat Primality Test

The first primality test that we considered was the Fermat primality test. Here is how this works. We begin with the number n that we wish to test for primality. We then randomly choose numbers less than n, say a and test the congruence

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

In other words we test to see if n divides $a^{n-1} - 1$. If we find that the answer is no, then we declare the number n composite. If not we continue with a different a. The choice of how many numbers a to test has to do with the size of n. For 300-digit numbers we use 10 such numbers. If the number n passes all the tests, then it is declared a *probable prime*. Thus this test is a probabilistic one.

Note that there are numbers that will pass the test for every $a < n$ which is coprime to n. Such numbers are called Carmichael numbers. Of course they will not pass the test if one chooses a number a which is not coprime to n, and thus the non-prime nature of n will be revealed. It is known that a Carmichael number is divisible by at least three distinct prime numbers and it is not divisible by the square of any prime number. The smallest Carmichael number is:

$$561 = 3 \cdot 11 \cdot 17$$

It is a very interesting theoretical fact that there exist infinitely many Carmichael numbers.

The Miller-Rabin Primality Test

The Miller-Rabin Test is a refinement of the Fermat Primality Test. Again we begin with a natural number n that we wish to test for primality. We randomly choose a number $a < n$. It can be made part of the process to test if a is coprime to n, because in the rare case that it is not, we can declare n composite right away. We then write:

$$n - 1 = 2^s \cdot u$$

Here we are assuming that n is an odd number and 2^s is the largest power of 2 that divides $n - 1$. Hence u is an odd number. We subsequently test consecutively the numbers:

$$a^u, a^{2u}, \ldots, a^{2^{s-1}u}$$

as to whether they are congruent to 1 or -1 modulo n. If we find one of them to be precisely that, then we stop the process and we declare n to have passed the test for the choice of a. If this condition fails for all the numbers then n is declared to be composite. As in the case of the Fermat primality test, we do this for a certain amount of choices that usually depend on the size of n. If the number n passes all the tests for all the choices of a's then we declare it a probable prime.

Overall the Miller-Rabin test is a very fast test, even though it is still considered to be a probabilistic test, yielding probable prime numbers and not numbers that are prime with 100% certainty.

The AKS Primality Test

Our main tool for establishing that a given number is prime with 100% certainty is the AKS primality test. This is named after Agrawal, Kayal and Saxena who discovered it in 2002. It is based upon the fact that for a natural number $n > 1$ and a coprime to n, then the polynomial relation:

$$(X + a)^n \equiv X^n + a \mod n$$

is true. This is a direct consequence of the Newton Binomial Theorem and of Fermat's Little Theorem. The point of the test is that the number n is prime if this relation holds for all numbers $a < n$ in a relatively small range.

Part of the test is to develop an algorithm that tests everything that is needed in order to establish the primality of a number according to the above theoretical fact. Note that the above relation can be thought of as a relation in the polynomial ring $\mathbb{Z}/n\mathbb{Z}[X]$.

It is quite instructive to try to apply this test in a naive way. What happens is that any reasonable time constraints are exceeded if we try to apply this theorem by actually computing powers of the corresponding polynomials. However there is a much faster algorithm, that we actually implemented in the pipeline that we will explain on the fourth column. This can be used in order to get primes in any range we like after we have applied all of our previous tools in order to arrive at numbers that are primes with high probability.

Our pipeline for finding large prime numbers

We combined all the theoretical facts that we have presented thus far, in creating a pipeline that finds prime numbers with hundreds of digits. Let's illustrate our pipeline as follows:

Find all primes in the trivial range
↓
Choose a range to look for primes
↓
Dismiss all multiples of primes in the trivial range
↓
Apply Fermat Primality Test to remaining numbers
↓
Apply Miller-Rabin Test to remaining numbers
↓
Apply AKS Test to remaining numbers

This yielded prime numbers such as:

```
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
```

We next wanted to play a little, based on a suggestion by Professor **Alexander Furman**. We used all the stages of the pipeline in order to construct a prime number with 1320 digits which conveys an actual picture. The number that we came up with passed the Miller-Rabin test and also passed the Baillie-PSW test which is essentially treated as deterministic in practice.

```
888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
888888888888888877777777777777777777777788888888877666666788888888888888888888888888888888888888888888888888888888888888
888888888888877654333333333333344445555666677766542122346788888888888888888888888888888888888888888888888888888888888888
888888888876543221111111111111111111222233333322211124567888888888888888888888888888888888888888888888888888888888888888
888888887653211111111111111000000000111110000000111246788888888888888888888888888888888888888888888888888888888888888888
888888765421012344455554321111223333333211100112346778888888888888888888888888888888888888888888888888888888888888888888
888888754333245667777776431234455666654211233455677888888888888888888888888888888888888888888888888888888888888888888888
888888754455667888898887531246778988764312467788888888888888888888888888888888888888888888888888888888888888888888888888
888888877778888888888765421357888975433224578888888888888888888888888888888888888888888888888888888888888888888888888888
888888888888888888887543322467888864212345688888888888888888888888888888888888888888888888888888888888888888888888888888
888888888888888888886311234578877642102467788888888888888888888888888888888888888888888888888888888888888888888888888888
888888888888888887654201357788865321113578888888888888888888888888888888888888888888888888888888888888888888888888888888
888888888888888876432112468887531111246888888888888888888888888888888888888888888888888888888888888888888888888888888888
888888888888887754201224578876531012346788888888888888888888888888888888888888888888888888888888888888888888888888888888
888888888888865422102356787643210135678888888888888888888888888888888888888888888888888888888888888888888888888888888888
888888888887653100113578887532110246788888888888888888888888888888888888888888888888888888888888888888888888888888888888
888888888754321002345788886421111357888987656667788888888888888888888888888888888888888888888888888888888888888888888888
888888765432111013567888888642111024566655443456778888888888888888888888888888888888888888888888888888888888888888888888
888888642100001235788888888642110001232211122467888888888888888888888888888888888888888888888888888888888888888888888888
888888653221123567888888888765432111112223456778888888888888888888888888888888888888888888888888888888888888888888888888
888888765444456788888888888877654433334445788888888888888888888888888888888888888888888888888888888888888888888888888888
888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
```

CAN YOU RECOGNIZE THIS NUMBER?