Primes in Sequences

By: Jae Young Lee

Project for MA 341 (Number Theory)
Boston University Summer Term I 2009
Instructor: Kalin Kostadinov

Jae Young Lee MA341 Number Theory

PRIMES IN SEQUENCES

HISTORY

A prime number is a natural number that can only be divisible by two distinct natural numbers: 1 and itself.

The history of prime numbers begins with the Ancient Greeks. A record of Euclid's Elements showed important theorems about primes and the fundamental theorem of arithmetic. Then in the 17th century another mathematician by the name Pierre de Fermat made a break thru in studying prime numbers with Fermat's Little Theorem (however at the time there was no proof of this theorem), and Fermat Numbers. After Fermat there comes many mathematicians that will further study the ideas of prime numbers the mystery of sequences containing only prime numbers.

There are many different types of prime number sequences. However the reason why that this topic still has yet to be fully understood is because even till this day there are only a finite number of primes known. A mathematician by the name Euclid came up with a theorem stating that there are infinitely many primes.

Proof (Euclid):

> *Consider any finite set of primes. Multiply all of them together and add 1 (see Euclid number). The resulting number is not divisible by any of the primes in the finite set we considered, because dividing by any of these would give a remainder of 1. Because all non-prime numbers can be decomposed into a product of underlying primes, then either this resultant number is prime itself, or there is a prime number or prime numbers which the resultant number could be decomposed into but are not in the original finite set of primes. Either way, there is at least one more prime that was not in the finite set we started with. This argument applies no matter what finite set we began with. So there are more primes than any given finite number. (Euclid, Elements: Book IX, Proposition 20*

Because there are infinitely many prime it takes a lot of time and expensive computers to come up with consecutively bigger prime numbers. Thus it is very hard to test a new

Prime number sequence without the proper intelligence. A fun fact: currently the largest prime number known is $2^{43,112,609}-1$, the number is a Mersenne prime (a prime in the 2^n-1 format). This number has nearly 13 million digits!

THEOREMS AND STANDARD SEQUENCES

Let us now further investigate the theorems behind prime sequences that are known today.

Fermat Numbers:

Fermat came up with the idea that all numbers with the form $F_n=2^{(2^n)}+1$ will always be a prime number. However this is only true till n=4, after that Euler later discovers that for n≥5 the numbers are all composite. The only known Fermat Primes are:

$F_0= 3$

$F_1= 5$

$F_2= 17$

$F_3= 257$

$F_4= 65537$

Thus a failed attempt in trying to create an infinite sequence containing only primes.

Mersenne Prime:

A monk named Mersenne studied the ideas of Fermat and tried coming up with another sequence with only primes. He came up with the formula (2^n)-1. However there are certain conditions.

$2^{ab} - 1= (2^a - 1)(1+2^a + 2^{a2a}+2^{3a}+\ldots+2^{(b-1)a})$

This identity shows that the number can only be prime if n is also a prime. Till this day Mersenne Primes are still being studied. As of 2009 there are only 46 known Mersenne Primes, one of them being the largest known prime number: $(2^{43,112,609} - 1)$. However the idea that Mersenne Primes will always be a prime number as long as n is a prime number is not true. For example for n=11, the number is 2047= 23x89.

Twin Primes:

Twin primes are prime numbers that have a difference on only 2, and because they come in pairs they are called twin primes. An example of twin primes are (3,5), (11,13)…etc. Just like Mersenne primes, it is still unknown if there are infinitely many twin primes. However it has been proven that every twin pairs except (3,5) comes in the form (6n-1, 6n+1) and n being any natural number, with the exception of n=1., n must end in 0,2,3,5,7, or 8. It is an easy proof to prove this. It has also been proven that a twin pair is a twin prime only if

$4((m-1)!+1) \equiv -m \pmod{m(m+2)}$. (However this proof is much harder to prove.)

The twin primes started a whole new chapter in prime sequences; the generalization is now prime numbers that have a difference of n, n being any natural number. For example sexy primes are prime numbers that have a difference of 6 between them.

Many more prime sequences can be found at: http://www.research.att.com/~njas/sequences/Sindx_Pri.html

It is clear that it is very hard to test if a sequence really contains only primes, however there are actual methods of verifying primality in a number or sequence. There are 6 main methods of testing if a number is really prime:

1. AKS primality test
2. Fermat primality test
3. Lucas primality test
4. Soloway-Stassen prilamity test
5. Miller-Rabin primality test
6. Elliptic cure primality proving.

Each of these tests play a big role on finding new prime numbers and eventually finding new prime sequences.

So after finding a prime number, what is their use? It may be surprising but prime numbers are a huge influence in the world of cryptography. Many public-key cryptography algorithms such as RSA or the Diffie-Hellman Key exchange. Prime numbers are also used in many theorems in the mathematical world. An example is the fundamental theorem of arithmetic, which stats that any positive integer greater than 1 can be written in a product of one or more primes. The proof of this theorem consists of two steps, the first to show that the every number is a product of zero or more primes; the second to show that any two representations may be joined into a single representation. Another surprising way prime numbers are used is in biology, specifically in DNA testing. Chains of DNA that only have genes that adds up to a prime number intrigue scientists. These chains seem to have a important impact on the human body, unfortunately many of them create a negative symptom on the body.

INVESTIGATION:

Since there are infinitely many primes and so much uncovered areas of prime sequences, anyone can further investigate this topic, and I have decided to do just that.

Lets take a set S, this set contains only natural numbers that are prime and have 11 as its last 2 digits; S= {211, 311, 811, 911, 1511…}. By studying a sequence like this, perhaps it can help us make a generalization of sequences like {277, 677, 977…}; sequences that contain only prime numbers and have a same two prime numbers as its last 2 digits. So to begin the investigation I studied the beginning digits of these numbers, since the last two digits will always be 11. (To the following numbers just add 11 to the end and you will get the numbers in set S). By doing this I noticed a pattern.

$2\equiv 2 \pmod 3$

$3\equiv 0 \pmod 3$

$8\equiv 2 \pmod 3$

$9\equiv 0 \pmod 3$

$15\equiv 0 \pmod 3$

$18\equiv 0 \pmod 3$

$20\equiv 2 \pmod 3$

$21\equiv 0 \pmod 3$

$23\equiv 2 \pmod 3$

$24\equiv 0 \pmod 3$

$27\equiv 0 \pmod 3$

$30\equiv 0 \pmod 3$

$35 \equiv 2 \pmod 3$

$39 \equiv 0 \pmod 3$

$41 \equiv 2 \pmod 3$

$42 \equiv 0 \pmod 3$

$50 \equiv 2 \pmod 3$

$57 \equiv 0 \pmod 3$

$60 \equiv 0 (\mathrm{mod}\ 3)$

$63 \equiv 0 \pmod 3$

$69 \equiv 0 \pmod 3$

$72 \equiv 0 \pmod 3$

$74 \equiv 2 \pmod 3$

$81 \equiv 0 \pmod 3$

All the numbers in set S are either 0 or 2 mod 3, and the form a certain pattern with the 0's and the 2's. There seems to be a pattern of (2,0,2,0) (0,0,0) (2,0,2,0) etc… Perhaps a pattern like this can be furthered studied to help us create a generalization of similar sequences such as this one.

SOURCES

http://primes.utm.edu/lists/small/10000.txt

http://www.research.att.com/~njas/sequences/Sindx_Pri.html

http://mathworld.wolfram.com/FermatPrime.html

http://en.wikipedia.org/wiki/Prime_number