Maths Internal Assesment

PROVING PRIME NUMBERS THEORIES AND USES

Proving Primes theories and uses

TABLE OF CONTENTS

A: There is no need for a table of contents for such a short piece of work.

Proving Primes theories and uses

INTRODUCTION

My interest on the investigation of prime numbers, came firstly from my math class when my teacher talked us about primes and some of their properties, being this numbers something fascinating having so many uses in our daily life and in the development of technologies all around the world, being these numbers the present but mainly the future of mankind. One of the comparison I like the most is that prime numbers are building blocks, just as atoms re to physic, prime numbers are to mathematics. A number is either a prime or it cambs broken down into product of primes. My teacher told me that these numbers where so beautiful because they are so complex we have not developed yet a formula that can give us all the prime numbers, being them so huge that not even the fastest computer could find this numbers in a fast way mainly because the latest prime found has 22,338,618 digits being this an absurd amount of digits. Additionally I interested in this topic because I think it would be a great help for developing my skills for paper 3 of this course. In my investigation I will focus on some hypothesis grate mathematicians have developed. Fermat´s little theories, and its expansion and proof developed by Euler known as Euler´s totient theorem being this connected with Carmichaels numbers and with Riemann Hypothesis, being all these theorems and hypothesis attempts to find a prime number formula. With the purpose of proving them and relating them with their uses, for demonstrating that math is present in almost everything we do.

The student's mother tongue is clearly not English. No penalties for language shortcomings, unless it is mathematical communication for instance, terminology in criterion B.

SIEVE ERATOSTHENES

Sieve Eratosthenes is one of the simplest´s ways of founding and listing prime numbers. It consists of writing a set of numbers (for example 1 to 100), where you need to select the first prime (2) and then search for all its multiples in all the set written. You continue doing this for all numbers and write apart the numbers that are not crossed out. You can evidence that all these numbers are going to be prime. The example for the first 120 numbers is:

4 de 11

B: The colours on this table do not help. It would have been better had all the non-primes been crossed out or the student had presented a legend to explain the colours.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime Numbers: 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, 101, 103, 107, 109, 113

As we can evidence in the table above, the numbers which are colorless, or not cross out are the prime numbers listed.
This method is very useful for founding and listing prime numbers but is not efficient due to the fact that if we try to do it in a larger scale (for example 10,000,000 terms), its going to take too much time to found list and verify each terms and each prime number found, being this method useful for a small amount of terms but being deficient in a larger scale

Proving Primes theories and uses

Fermat´s Little Theorem

Fermat´s little theorem is one test that can help us find prime numbers using the formula

$$a^{P-1} = 1 \pmod{P}$$

where P is a prime number
A is an integer which is nos multiple / divisible by P

B: Should not be capitalized. The student should also explain the notation used, for instance, modular arithmetic.

This theorem can be proved by mathematical induction in the following way:

1. We need to take two numbers A and P which are going to be relatively prime and P being a prime.
2. take into consideration the multiples of A = [a, 2a, 3a, 4a, 5a ..... (p-1)a]
3. We consider the set of values [1, 2, 3, 4, 5 … (p-1)]
4. If we take the product of these two sets we obtain: [a x 2a x 3a x 4a x 5a ...(p-1)a] and [1 x 2 x 3 x 4 x 5 … (p-1)] (each element on the first set of numbers has a congruence to an element in the second set)
5. As a consequence [a x 2a x 3a x 4a x 5a ...(p-1)a] = [1 x 2 x 3 x 4 x 5 … (p-1)] (mod p)
6. Factorize the term a^{P-1}

B: It is not clear what this is?

7. we are left with [a x 2a x 3a x 4a x5a … (p-1)a] = [1 x 2 x 3 x 4 x 5 … (p-1)] (mod P) ???
8. Divide each sibe by [1 x 2 x 3 x 4 x 5 ..... (p-1)] (remember P must be a prime number)

9. We obtain $a^{P-1} = 1 \pmod{P}$

in summary we can said that " If P is a prime and A is any integer not divisible by P, then A ^ P-1 is divisible by P " (Fermat)

B: Should be in same line. Incorrect notation.

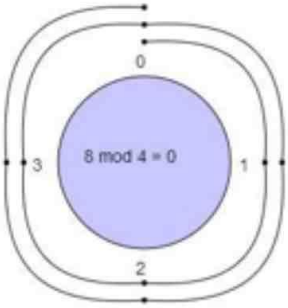
For understanding this theorem its necessary to understand modular arithmetic.

One easy example of modular arithmetic is this type of division:
11/3 = 3 R= 2 which can be written as : 11 = 2 mod 3

A: This should have come before the theorem.

or 23/3 = 7 R= 2 which can also be written as 23 = 2 mod 3
One of the most common graphic representations of Modular arithmetic is a clock as the following example.

Proving Primes theories and uses



In this case we are finding 8 mod 4.
First is needed to draw a clock, and as we have mod 4, we use the first four integers (0, 1, 2, 3)

E: This is incorrect.

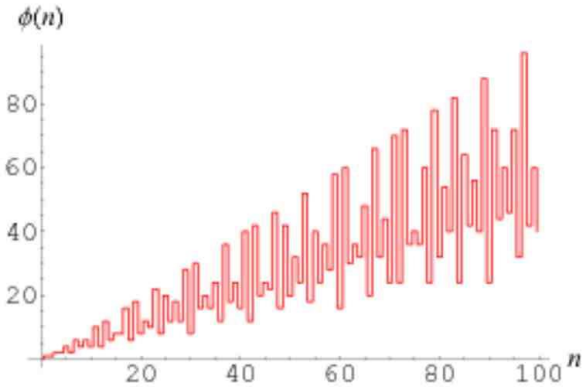
We start form 0 and give 8 rounds, being each number one round.
After the 8 rounds she end up in cero. Meaning that 8 mod 4 = 0
Tip: If the modulus is positive we count clockwise if its negative anti-clockwise.

Modular arithmetic is one important part of the technological development, due to the fact that it is used in programming language.

Proving Primes theories and uses

Euler´s totient theorem

We can evidence how Fermat´s little theorem is related to Euler´s totient theorem, being Fermat´s theorem an special case of what Euler stated on his theorem.



"The totient function $\phi(n)$, also called Euler's totient function, is defined as the number of positive integers $\leq n$ that are relatively prime" [1]

Totient Theorem can be prove in a similar way as we did with Fermat´s theorem and we need to follow these steps reaching the formula the theorem states $a^{\phi(n)} \equiv 1 \pmod{n}$

E: According to this there are phi(n)+1 elements.

1. We need to take two numbers A and n which are going to be relatively prime
2. Take into consideration the set of numbers N which are relative prime to n [1, n1, n2… $n_{\Phi n}$] (This set of numbers will have Φn amount of number)
3. Notice the set of numbers aN, Where we fin de product of a and N [a, an1, an2, an 3 … $an_{\Phi n}$]
4. The elements in both sets will be congruent one to each other, as a consequence both of the sets are gong to be congruent
5. In consequence, [a x an1 x an2 x… x $an_{\Phi n}$] = [1 x n1 x n2 x…x $n_{\Phi n}$] (mod n)
6. Factorize the term a ^ Φn
7. a ^ Φn [1 x n1 x n2 x ... x $n_{\Phi n}$] = [1 x n1 x n2 x ... x $n_{\Phi n}$] (mod n)
8. We divide in bot sides by [1 x n1 x n2 x ... x $n_{\Phi n}$] when all the elements are relative primes to n
9. we finally get $a^{\phi(n)} \equiv 1 \pmod{n}$ hence proving this theorem.

B: Consistent use of ^ for power.

[1] http://mathworld.wolfram.com/TotientFunction.html

Applications

In mathematics, we can see how these two theorems are very important not only to the facts that they are relevant when attempting to find prime numbers, but also we can see how both of these theorems are used to solve non-linear equations.
Additionally, in the modern life both of these theorems are used mainly in digital security being prime numbers, thus this theorems in the encryption of information, being these codes difficult to solve.

D: This is an attempt to reflect on the significance of these theorems but it is poorly done.

Carmichael Numbers - Pseudo Primes

Charmichael numbers are some numbers that are considered pseudo primes (probable prime numbers that are not actually prime numbers. They are classified according to the properties each one of them fulfill) because even though they are not prime numbers they full fill the conditions imposed by Fermat´s little theorem like if they where really primes.
Some Carmichael numbers are 1729, 561, 1105, 2465.
"Numbers of the form $(6k+1)(12k+1)(18k+1)$ are Carmichael numbers if each of the factors is prime"[2]

B: It is unclear what is being said here.

PROPERTIES OF CARMICHAEL NUMBERS

1. If a prime p divides the Carmichael number n, then $n \equiv 1 \pmod{p-1}$ implies that $n \equiv p \pmod{p(p-1)}$.
2. All Carmichale numbers are square free (if its prime decomposition contains no repeated factors. All primes are therefore trivially squarefree.[3]) meaning that it is at least a product of three different primes.

We can see how these special numbers are related to the primes theories we have explained previously due to the fact that the act like if they where prime numbers even though they are not. With this in mind we know that Carmichael numbers pass Fermat´s test accomplishing the formula of Fermat´s little theories and Euler´s totient formula.

A, E: Here the candidate is simply quoting properties of Carmichael numbers without explaining what they are; penalty in E, not in A.

[2] http://mathworld.wolfram.com/CarmichaelNumber.html

[3] Squarefree. (n.d.). Retrieved March 14, 2017, from http://mathworld.wolfram.com/Squarefree.html

Proving Primes theories and uses

$n^2 + n + 41$ formula

This formula is one of the attempts used to find prime numbers and it is very useful, the only problem is that we can observe that unit number 38, we can deduce / produce prime numbers, but after this number (38) the pattern breaks and no longer primes can be deduced being this one of the biggest limitations mathematicians have had when finding primes .

E: Why at 38?

one example of how this formula works is for example if we plug in any number in the range of 1 - 38

5^2 + 5 + 41 = 71 which is a prime number.

Mersenne primes

Mersenne primes are numbers that are expressed in the form of (2^p) -1 for when this expression is a prime them P will be a prime number.

one example of this is if the plug in p=2

(2^2)-1 = 3 as we can see, 3 that is the result of the operation is a prime number, thus, 2 (p) is also a prime number.

Prime numbers theorem

Prime number theorem tries to answer one of the most important questions when referring to prime numbers and to mathematics in general. These two questions are how many primes are there ? and how big is the n prime? With this purpose, prime number theorem tries to give a formula for expressing and finding all prime numbers, something that until now has been impossible.
For now, prime number theorem is limited to give an estimate. The number of primes that are less or equal to n are written as π (n), where there is not relationship with the significance of π in the context of a circle.
Its safe to said that excepting prime numbers 2 and 3, all the other prime numbers are in the form of 6n ± 1, concluding that more or less one third of all numbers are going to be prime, but this is not completely satisfying, being there also prime numbers in the form of 30 ± 1, 30 ± 7, 30 ± 11 or 30 ± 13.
Prime number theorem states that as n is increased, the value of π(n) asymptotically is approached to n/log (n), meaning that π(n)/ n / log(n) tends to cero when n tends to infinity.

A: Not clearly explained at all, and this is not because of language.

Proving Primes theories and uses

This part of the theorem, states one of the most aceptable and exact approaches for mathematicians to know and answer the questions that are state previously. With this theorem, its possible to approach how many prime numbers are there and how big is it going to be, being until now 22,338,618 digits the biggest prime number found.

CONCLUSIONS

Finally, we can conclude that prime numbers are one of the most amazing thing in the mathematics world, because they seem to be so simple but actually the are on the contrary one of the most serious and difficult topics in math, as we can evidence that there is not a formula that can give us all the prime numbers, or even tell us how many are there exactly.
Additionally, we can affirm that even though there is not an exact formula for finding prime numbers there have been gray mathematicians such as Euler or Fermat, that had create theorems that approach us, and take us one step closer for finding the answer to all the question we have about this numbers and personally I think that they take us one step closer to understand the future and the new technologies we can developed based on this numbers.
Even more, we can evidence how there have been even more advances, such us the prime number theorem that can give us a fair estimate of how many primes are there and which one is the the biggest prime possible.
Finally, in my personal opinion I think that this numbers are the key for the future and for many advances we can not even imagine. This topic of prime numbers, is one of my favorite topics due to the collateral beauty we can see on them, being prime numbers one of the most challenging topics mathematicians have been working for many decades. Additionally, this work has give me more arguments and knowledge to face the end of my high school stage and the challenges, math class might bring.

BIBLIOGRAPHY

Inductive proof of Fermat's little theorem proof. (n.d.). Retrieved March 14, 2017, from http://planetmath.org/inductiveproofoffermatslittletheoremproof

M. (2015, November 22). Fermat's Little Theorem examples. Retrieved March 14, 2017, from https://www.youtube.com/watch?v=pMA-dD-KCWM

https://primes.utm.edu/notes/proofs/FermatsLittleTheorem.html

Fermat's little theorem. (n.d.). Retrieved March 14, 2017, from https://www.khanacademy.org/computing/computer-science/cryptography/random-algorithms-probability/v/fermat-s-little-theorem-visualization

Khan Academy. (n.d.). Retrieved March 14, 2017, from https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/what-is-modular-arithmetic

Carmichael Number. (n.d.). Retrieved March 14, 2017, from http://mathworld.wolfram.com/CarmichaelNumber.html

Proving Primes theories and uses