MATHS COURSEWORK

Proving Euler's Totient Theorem

TABLE OF CONTENTS

Proving Euler's Totient Theorem

MATHS COURSEWORK

Proving Euler's Totient Theorem

Introduction

My interest in Euler as a mathematician was first sparked when, on completing a listener crossword, the hidden message "Read Euler, he is the master of us all" was revealed, so when I saw the inclusion of his name on the list of prompt words there was really no option but to go for him. Euler was a mathematician in the 18th century and is responsible for the first proofs of many great many number of conjectures and problems. In number theory alone his accomplishments include proving the two square theorem and Fermat's little theorem as well as doing a great deal of work that later led to the first proof of the four square theorem. His achievement that I am going to focus on though is less well known, it is a generalisation of Fermat's little theorem that has come to be known as Euler's totient theorem.

The Theorem

Euler's totient theorem[1] states that for relatively prime a and n:

$$a^{\Phi n} \equiv 1 \pmod{n}$$

Where Φn is Euler's totient function

Euler's Totient Function

Euler's totient function[2], or Φn, is a count of the numbers that are less than n and relatively prime to n. For example Φ_{10} is 4 as there are four number less than ten that are relatively prime to 10 { 1, 3, 7, 9 }, Φ_{11} is 10 as 11 is prime all numbers less than it are relatively prime to it and Φ_6 is 2 as 1 and 5 are relatively prime to 6 but 2,3 and 4 are not.

---

[1] http://en.wikipedia.org/wiki/Euler's_theorem

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

Below is a table of the totients of the numbers up to 20.

N	Φ_N
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

Some examples will serve to demonstrate Euler's totient theorem.

Let $n = 10$ and $a = 3$. Note that 10 and 3 are relatively prime. From the table $\Phi_{10} = 4$. Then, $3^4 = 81 \equiv 1 (\text{mod } 10)$.

Also, if $n = 15$ and $a = 2$ we see that $2^8 = 256 \equiv 1 \ (\text{mod } 15)$.

Fermat's Little Theorem

Euler's totient theorem is a generalisation of Fermat's little theorem[3] and works for all n relatively prime to a. Fermat's little theorem only works for a and p relatively prime

[3] http://mathworld.wolfram.com/FermatsLittleTheorem.html

Proving Euler's Totient Theorem

where p is itself prime and states:

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

or

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

It is immediately apparent that this fits in with Euler's totient theorem for primes p, as we have seen Φp, where p is a prime, is always p-1.

As an introduction to Euler's totient theorem I shall prove Fermat's little theorem.

Proving Fermat's Little Theorem

RTP: $a^p \equiv a \pmod{p}$

Take two numbers a and p which are relatively prime, and where *p* itself is prime.

Consider the set of the multiples of a { a, 2a, 3a, 4a, 5a ..... (p-1)a }

Consider the set of numbers { 1, 2, 3, 4, 5 ..... (p-1) }

If taken to the modulus p each element of the first set will be congruent to an element in the second, there will be one to one correspondence between the two sets and this is proven as lemma 1.

If we take the product of the first set { a x 2a x 3a x 4a x 5a ..... (p-1)a } and the product of the second { 1 x 2 x 3 x 4 x 5 ..... (p-1) } we can see that they are congruent to one another (as each element in the first is congruent to an element in the second)

Therefore { a x 2a x 3a x 4a x 5a ..... (p-1)a } $\equiv$ { 1 x 2 x 3 x 4 x 5 ..... (p-1) } (mod p)

We can take out a factor of a^{p-1} from the left hand side

Giving a^{p-1} { 1 x 2 x 3 x 4 x 5 ..... (p-1) } $\equiv$ { 1 x 2 x 3 x 4 x 5 ..... (p-1) } (mod p)

By dividing each side by { 1 x 2 x 3 x 4 x 5 ..... (p-1) } which is valid as p is prime we get

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

or

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

QED.

Proving Euler's Totient Theorem

Lemma 1: Each number in the first set must be congruent to one and only one number in the second and each number in the second set must be congruent to one and only one number in the first. This may not be obvious at first but can be proved through three logical steps.

(1) Each number in the first set must be congruent to one of the elements in the second as all possible congruences save 0 are present, none will be congruent to 0 as a and p are relatively prime.

(2) A number cannot be congruent to two numbers in the second set as a number can only be congruent to numbers which differ by a multiple of p, as all elements of the second set are smaller than p a number can only be congruent to one of them.

(3) No two numbers in the first set, call them ba and ca, can be congruent to the same number in the second. This would indicate that the two numbers were congruent to each other $ba \equiv ca \pmod{p}$ which would indicate that $b \equiv c \pmod{p}$ which is not true as they are both different and less than p itself.

Therefore, through these three steps Lemma 1 is proven.

Proving Euler's Totient Theorem

As Fermat's little theorem is a special case of Euler's totient theorem (where n is prime) the two proofs are quite similar and in fact only slight adjustments need to be made to the proof of Fermat's little theorem to give you Euler's totient theorem[4].

RTP: $a^{\Phi n} \equiv 1 \pmod{n}$

Take two numbers, a and n which are relatively prime

Consider the set N of numbers that are relatively prime to n $\{ 1, n_1, n_2 ... n_{\Phi n} \}$

This set will have Φn elements (Φn is defined as the number of numbers relatively prime to n)

Consider the set aN, where each element is the product of a and an element of N $\{ a, an_1, an_2 ... an_{\Phi n} \}$

Each element in set aN will be congruent to an element in set N (mod n), this is follows by the same argument as in lemma 1 and so the two sets will be congruent to each other

Therefore $\{ a \times an_1 \times an_2 \times ... \times an_{\Phi n} \} \equiv \{ 1 \times n_1 \times n_2 \times ... \times n_{\Phi n} \} \pmod{n}$

[4] http://planetmath.org/?op=getobj&from=objects&id=335

Proving Euler's Totient Theorem

By taking out a factor of $a^{\Phi n}$ from the left hand side we get

$a^{\Phi n} \{ 1 \times n_1 \times n_2 \times ... \times n_{\Phi n} \} \equiv \{ 1 \times n_1 \times n_2 \times ... \times n_{\Phi n} \} \pmod{n}$

If we then divide through by $\{ 1 \times n_1 \times n_2 \times ... \times n_{\Phi n} \}$ which is valid as all elements are relatively prime to n we get

$$a^{\Phi n} \equiv 1 \pmod{n}$$

QED.

Applications

Unlike some of Euler's other work in number theory such as his proof of the two square theorem Euler's totient theorem has very real uses and applications in the world and like much of number theory those uses are almost exclusively in the world of cryptography and cryptanalysis. Both Fermat's little theorem and Euler's totient theorem are used in the encryption and decryption of data, specifically in the RSA encryption system[5], whose protection revolves around large prime numbers raised to large powers being difficult to factorise.

Conclusion

This theorem may not be Euler's most elegant piece of mathematics (my personal favourite is his proof of the two square theorem by infinite descent) or at the time seemed like his most important piece of work at the time but this, in number theory at least, is probably his most useful piece of mathematics to the world today.

This proof has given me a chance to link up some of the work I have done in the largely separate discrete mathematics and sets relations and groups options. These two options appear to me to be the purest sections of mathematics that I have studied but are for whatever reason seldom linked in class, this project has allowed me to explore the links between them and use knowledge from one in relation to the other, broadening my view of maths.

[5] http://www.muppetlabs.com/~breadbox/txt/rsa.html#7

Proving Euler's Totient Theorem