THE EULER-FERMAT THEOREM AND GROUP THEORY

DANIEL MATHEWS

The aim is to prove the following theorem:

Theorem 0.1. *If $(a,n) = 1$ then $a^{\phi(n)} \equiv 1$ (mod n) where $\phi(n)$ is the Euler phi function, ie the number of positive integers less than n which are relatively prime to n.*

Lemma 0.2. *Let the elements of $\{1, 2, \ldots, n\}$ which are relatively prime to n, be denoted as S. Then, under multiplication modulo n, S forms a group under multiplication.*

Recall that proving S is a group just means proving three things:

(i) *If $a, b, \in S$ then $ab \in S$ (the* closure *requirement).*
(ii) *There is an element $e \in S$ such that for all $a \in S$, $ae = ea = a$ (the* identity *requirement).*
(iii) *If $a \in S$ then there is an element denoted $a^{-1} \in S$, called the inverse of a, such that $aa^{-1} = a^{-1}a = e$, the identity (the* inverse *requirement).*

Before going on, note that, in dealing with multiplication modulo n, obviously it is true that $ab = ba$ — ie the group is *commutative*. We cannot make this assumption with groups in general, though.

Proof. (i) If a, b are relatively prime to n, then ab is relatively prime to n — simply consider their prime factorisations. Any prime appearing in the factorisation of n cannot appear in a or b, hence not in ab.

Further, the property of 'being relatively prime to n' is preserved upon adding/subtracting multiples of n — this is part of the Euclidean algorithm. So ab, modulo n, will be a member of S.

(ii) This is obviously true if we take $e = 1$ (modulo n). (Hereafter we will write 1 instead of e)

(iii) Take any $a \in S$. Since $(a,n) = 1$, we know that there exist x, y such that $ax + ny = 1$ (Euclidean algorithm). But then $ax \equiv 1$ (mod n), so x is an inverse for a.

□

Definition 0.3. The *order* of an element a in a group G is the least $n \in \mathbb{N}$ such that $a^n = 1$.

Lemma 0.4. *$a^m = 1$ iff m is a multiple of the order of a.*

Proof. Let n be the order of a. So $a^n = 1$ and for a positive integer k

$$a^{kn} = \overbrace{a^n a^n \cdots a^n}^{k \text{ times}} = \overbrace{1 \cdot 1 \cdots 1}^{k \text{ times}} = 1$$

Date: February 2002.

Hence if m is a multiple of n, then $a^m = 1$.

For the converse, consider the sequence $1, a, a^2, \ldots, a^n, a^{n+1}, \ldots$.

Since $a^n = 1$, and is the least power to do so (by the definition of order), we have $a^n = 1$, $a^{n+1} = a$, $a^{n+2} = a^2$, and so on. In general $a^{kn+l} = a^l$. That is, the sequence cycles exactly every n elements, and no more often.

If some $a^m = 1$ but m is not a multiple of n , then there must be some $m' \leq n$ with $a^{m'} = 1$. This is a contradiction. □

Having set up a couple of group-theoretic ideas, we now prove a more general theorem relating the order of an element to the size of the group. This is *Lagrange's theorem* and actually extends to all subgroups of a group.

In thinking about elements and their orders, perhaps a good example is the integers modulo 11, and the group consisting of the relatively prime integers 1,2,3,4,5,6,7,8,9,10 ($\phi(11) = 10$) under multiplication modulo 11. For instance, if we look at $1, 4, 4^2, \ldots$ we find that $4^5 = 1$, but if we take the sequence 2^k we find the order of 2 is 10. Similarly the order of 10 is 2 and the order of 1 is 1. So bear that in mind while reading the theorem and its proof...

Theorem 0.5 (Lagrange's Theorem)**.** *Let G be a group with m elements and let $a \in G$. Then the order of a is a factor of m.*

Proof. Let the order of a be n.

Define $x, y \in G$ to be *equivalent*, denoted $x \sim y$, if $xy^{-1} = a^k$ for some integer k, ie $x = a^k y$. This relation divides G up into classes of equivalent elements — and each element of G is in some equivalence class (even if it is the only element in its class!).

The trick is to show all the equivalence classes are the same size (if you try a few examples, such as modulo 11, you will quickly find this is the case). So we have a lemma.

Lemma 0.6. *Every equivalence class is a set of the form*

$$\left\{x, xa, xa^2, \ldots, xa^{n-1}\right\}$$

for some particular $x \in G$ and where n is the order of a.

Proof. Take an equivalence class E and an element x in it. Then every element y of E satisfies $x \sim y$, that is $y = xa^k$. But now $xa^k = xa^l$ iff $x^{-1}xa^k = x^{-1}xa^l$, ie $a^k = a^l$, ie $a^{k-l} = 1$, so $k - l$ is a multiple of n.

So $\{x, xa, xa^2, \ldots, xa^{n-1}\}$ are all distinct, and any other element xa^k is equal to one of these elements.

Hence the equivalence class is as claimed. □

Corollary 0.7. *Every equivalence class has the same number of elements, n, the order of a.*

Returning to the proof of Lagrange's theorem, we see that the group G is divided into equivalence classes with n elements. Hence the total number of elements in the group m is a multiple of n.

So the order of a is a factor of m, as required. □

From Lagrange's theorem, the Euler-Fermat theorem falls out.

Corollary 0.8. *Take a group G with m elements and $a \in G$. Then $a^m = 1$.*

Proof. Let n be the order of a. Then n is a factor of m be Lagrange's theorem, so by Lemma 0.4, $a^m = 1$. □

Now we can easily prove the Euler-Fermat theorem! The group of elements relatively prime to n, under multiplication modulo n, forms a group. The number of elements in the group is $\phi(n)$. So if $(a, n) = 1$, then a is a member of the group, and by the above corollary, $a^{\phi(n)}$ is equal to the identity element, which means

$$a^{\phi(n)} \equiv 1 \bmod n.$$