ALL FINITE FIELDS HAVE A PRIME-POWER ORDER

MORPHISMS, CAUCHY'S THEOREM, AND PROOF OF THEOREM
Daniel R. Page, 2011 (Updated December 20, 2012)

Morphisms are a powerful tool in proving properties of mathematical objects because it provides a technique to develop one mathematical object from another mathematical object. These are a core study in *Category Theory* but are applied in algebraic fields from *Group Theory*, to *Universal Algebra* (so there is a lot of breadth to where morphisms are used). We will cover the very basics of morphisms. Following this we will state *Cauchy's Theorem*, which is closely related to Lagrange's Theorem. Then we will prove this claim involving the order of all finite fields.

DEFINITIONS:
Group: Recall, a Group G is a non-empty set with a binary operation '·', such that we have the following axioms:

- Closure: For any $x, y \in G$, $x \cdot y \in G$.

- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ For all a,b,c $\in G$

- Identity: There exists an element $e \in G$ such that for any element $a \in G$, $a \cdot e = e \cdot a = a$.

- Inverses: For each element $x \in G$, there exists an element $y \in G$ such that, $x \cdot y = y \cdot x = e$.

A Group is called *Abelian* when we include the *axiom of commutativity*. That is, for any elements $a, b \in G$, $a \cdot b = b \cdot a$.

Homomorphism: A function α that takes a set of elements of one group G to the set of elements of another group G' while preserving the group operation '·'. A homomorphism α is denoted by $\alpha : G \to G'$. Given two groups $(G, \cdot)$ and $(G', +)$, a function α is called a *homomorphism* if and only if $\alpha(a \cdot b) = \alpha(a) + \alpha(b)$.

Example: Suppose we have two *Abelian* groups G, and G'. In particular, let us be interested in addition (so both G and G' will have the additive operator '+'). Observing by the properties of an Abelian group, notice we have commutativity along with closure. This implies under addition there exists a *homomorphism* γ, such that $\gamma : G \to G'$. This is strict because $\gamma(a + b) = \gamma(a) + \gamma(b)$ where a and b are elements in G'. Even more useful, γ will give us another abelian group by the axioms of an abelian group. Infact, an abelian group homomorphism is an *automorphism*.

Automorphism: A type of *homomorphism* where a function α is a bijective mapping of a group G onto itself where α permutes the elements of G. An automorphism α is denoted by $\alpha : G \to G$.

Example: Given a *cyclic group* $G = C_p = \{g | g^p = 1\}$ where g is the generator, then there exists an automorphism in G, say α so that $\alpha : C_p \to C_p$. That is $\alpha(g) = g^k$ where $k \in \mathbb{Z}_p$. *Note: k=1 gives the same cyclic group because* $\alpha(g) = g$.

Example: Let us look at $GF(2^2)$. Say if one were to take any two non-zero elements in $GF(2^2)$, say a, b. By the closure axiom in finite fields, we should get another element that is in $GF(2^2)$. This implies that there exists an automorphism λ such that $\lambda : GF(2^2) \to GF(2^2)$. This means given any two elements in a galois field, we will obtain a permutation of the elements if we were to fix one of the elements. If we exhaust all possible pairs we will obtain a *latin square* as our addition table (or list of functions in terms of one element). We observe the same property in multiplication providing we have a prime-power for the order of our galois field along with the same property with the multiplication table respectively.

THEOREM - CAUCHY'S THEOREM: If G is a finite group and p is a prime number that divides the order of G, then G contains an element of order p. *This means that there will exist $x \in G$ where p is the lowest non-zero integer where $x^p = e$ where e is the identity element.*

THEOREM: All finite fields have a prime-power order.

Proof:
Let F be a finite field and $a, b \in F/\{0\}$. Suppose we have a function f which *sends a to b*. Note that f would preserve the additive property of F because additive closure is held in F. We will draw our attention to the addition operation of the field F. If we focus on '+', then F is a finite abelian group α where we have $a, b \in F/\{0\}$ in α. Since these elements are under the same domain under F and α, this implies there is an *automorphism* of α such that $f : F/\{0\} \to \alpha$. Now that there is a correspondence between a finite field F and a finite abelian group α. We wish to show that for any abelian group α that has an automorphism of α between any two non-zero elements that the order of α is a prime-power. We need to consider the trivial abelian group, and the non-trivial abelian groups.
Case 1: The trivial abelian group has order 1, which holds for any prime p because, $p^0 = 1$.
Case 2: Now, we wish to show that for any non-trivial abelian group α that has an *automorphism* of α that has an order that is a prime-power. Suppose p is a prime factor of the $|\alpha|$ (the order of α). By the *unique factorization theorem*, $|\alpha| = \prod_{i=0}^{k} p_i^{e_i}$, where $p_i \in \mathbb{P}$ and $e_i \in \mathbb{N}$. If the order of α were to

be a prime-power, then there does not exist $q \in \mathbb{P}$, such that $|\alpha| = q^{k_1} p^{k_2}, p \neq q$.

Assume a q does exist such that, $|\alpha| = q^{k_1} p^{k_2}, p \neq q$. By *Cauchy's Theorem*, we can state that there is an element $a \in \alpha$ of order p. By our assumption that there is an automorphism f of α such that f(a) = b where b is non-zero by the definition of an abelian group. Since for any element in under the domain of f there is an *automorphism* for each member of the group α, b has an order p too! This means all non-zero elements in α have an order p.

By our assumption, assume we were to divide the size of α by q. *Cauchy's Theorem* states there is an element in α of order q. Unfortunately for our assumption, we already showed that all non-zero elements in α have an order p. So $p = q$. This arises in a contradiction! This implies that the only prime factor of the order of α is p. Thus, the non-trivial abelian group α has a prime-power order. By the automorphism of α from our finite field, F has a prime-power order too.

Therefore, all finite fields have a prime-power order. $\square$

REFERENCES
[1] Walter Ledermann, Alan J. Weir, Introduction to Group Theory, Addison Wesley Longman, 1997
[2] Eliakim H. Moore, The subgroups of the generalized finite modular group, University of Chicago Press, 1903