From Mathematics to Generic Programming

Brooks Mershon

March 2017

6.10

Solution.

Any group G of prime order p must have as its subgroups $\{1\}$ and G, otherwise we would find a contradiction with Lagrange's Theorem: *the order of any subgroup H of a finite group G divides the order of that group.*

Let a be an element other than the identity element in G. The order of a must be $p = |G|$, by the above reasoning. The order of the identity element is 1, and that is the only element which can have order 1 (otherwise that other element must be the identity element). If the order of an arbitrary a in G is the order of the group itself, then we must be able to find some $m \geq 0$ such that $b = a^m$ for any $b \in G$. That is, G is a cyclic group. We would not be able to prove this if we couldn't draw upon Lagrange's Theorem and our knowledge of the primality of the order of G; if the order of G were not prime, we could not guarantee that a would not have an order less than n, and further, we could not guarantee that some a exists for which every $b \in G$ is reachable by some power of a.