Problem C NAW 5/7 nr. 4 december 2006

Jaap Spies

December 2006

The problem

Introduction

Let G be a finite group of order $p+1$ with p a prime. Show that p divides the order of $Aut(G)$ if and only if p is a Mersenne prime, that is, of the form 2^n-1, and G is isomorphic to $(Z/2)^n$.

Solution

Let p be a Mersenne prime with $p = 2^n - 1$ and G be isomorphic to $(Z_2)^n$, so G is an elementary Abelian group of order 2^n. It is a well known fact that the group of automorphisms of the elementary Abelian group of order q^r is of order $(q^r-1)(q^r-q)...(q^r-q^{r-1})$, the order of $GL(r,q)$. Hence $p = 2^n-1$ is a divisor of $|Aut(G)|$.
Let now p be a divisor of $|Aut(G)|$. $|G| = p+1$, so there are p elements of G not equal the identity e, say $g_1, g_2, ..., g_p$. Clearly $p > 2$, so $p+1$ is even, so according to the first Sylow Theorem there is a subgroup of G of order 2, and hence there is an element g of order 2. As p is a divisor of the order of the automorphism group of G, we need all possible automorphisms with $g \to g_i$, $i = 1, 2, ..., p$, hence all elements g_i are of order 2.
So G is isomorphic to $(Z/2)^n$ with $p+1 = 2^n$ and hence $p = 2^n-1$ is a Mersenne prime.