Campo Galois $GF(p^r)$

Resumen

1. Sea F un campo con q elementos y a un elemento no nulo de F. Si n es el orden de a, entonces $n|(q-1)$.
2. Sea p primo y $m(x)$ un polinomio irreducible de grado r en $Z_p[x]$. Entonces la clase residual $Z_p[x]/\equiv_{m(x)}$ es un campo con p^r elementos que contiene Z_p y una raíz de $m(x)$.
3. Sea F un campo con q elementos. Entonces $q = p^r$ con p primo y $r \in N$

velos