generator for the mutiplicative group of a field

Canonical name	GeneratorForTheMutiplicativeGroupOfAField
Date of creation	2013-03-22 16:53:17
Last modified on	2013-03-22 16:53:17
Owner	polarbear (3475)
Last modified by	polarbear (3475)
Numerical id	16
Author	polarbear (3475)
Entry type	Result
Classification	msc 11T99
Classification	msc 12E20

Proposition 1 *The multiplicative group K^* of a finite field K is cyclic.*

Theorem 3.1 in the `http://planetmath.org/FiniteField`finite fields entry proves this proposition along with a more general result:

Proposition 2 *If for every natural number d, the equation $x^d = 1$ has at most d solutions in a finite group G then G is cyclic. Equivalently, for any positive divisor d of $|G|$.*

This last proposition implies that every finite subgroup of the multiplicative group of a field (finite or not) is cyclic.
We will give an alternative constructive proof of Proposition 1:
We first factorize $q-1 = \prod_{i=1}^{n} p_i^{e_i}$. There exists an element y_i in K^* such that y_i is not root of $x^{(q-1)/p_i} - 1$, since the polynomial has degree less than $q-1$. Let $z_i = y_i^{(q-1)/p_i^{e_i}}$. We note that z_i has order $p_i^{e_i}$. In fact $z_i^{{p_i}^{e_i}} = 1$ and $z_i^{{p_i}^{e_i-1}} = y_i^{(q-1)/p_i} \neq 1$.
Finally we choose the element $z = \prod_{i=1}^{n} z_i$. By the Theorem 1 `http://planetmath.org/OrderOfEl`
we obtain that the order of z is $q-1$ i.e. z is a generator of the cyclic group K^*.