

THE PRIMITIVE ELEMENT THEOREM

April 15, 2008

Primitive Element Theorem. *Let F be a finite field, and let U be its set of units, the non-zero elements of F . Let $n = |U|$, the number of elements in U (so that $n = |F| - 1$). Then U has an element whose order is n .*

Such an element is called a “primitive element” for F . If u is a primitive element of F , then we know that the elements $1, u, u^2, \dots, u^{n-1}$ are all distinct, so every element of U is a power of u . The following two lemmas are crucial ingredients in the proof of the Primitive Element Theorem:

Lemma 1. *Let U be as above, and let x and y be elements of U , with orders s and t , respectively. If s and t are relatively prime, then xy has order st .*

Proof. Let r be the order of xy . We note that $(xy)^{st} = x^{st}y^{st} = (x^s)^t(y^t)^s = 1^t1^s = 1$; therefore $r \mid st$.

We have $1 = (xy)^r = x^r y^r$, so $x^r = y^{-r}$. The order p of x^r is $\frac{s}{\text{GCD}(r,s)}$, so, in particular, $p \mid s$. Since p is the order of y^{-r} , we have $p = \frac{t}{\text{GCD}(-r,t)}$, so, in particular, $p \mid t$. Since s and t are relatively prime, $p = 1$. We have shown that $x^r = 1$. The equation $x^r = y^{-r}$ shows that $y^{-r} = 1$, and it follows that $y^r = 1^{-1} = 1$. Therefore $s \mid r$ and $t \mid r$. Since s and t are relatively prime, $st \mid r$. Since we already showed that $r \mid st$, it follows that $r = st$. \square

PET1. Let $F = \mathbb{Z}/31\mathbb{Z}$, and let U be the set of units of F .

- (a) Find the order of 2.
- (b) Find the order of 5.
- (c) Find an element of order 15.
- (d) Find an element of order 2.
- (e) Find a primitive element for F .

PET2. Let $F = \mathbb{Z}/73\mathbb{Z}$, and let U be the set of units of F .

- (a) Show that 2 has order 9.
- (b) Show that 21 has order 24.
- (c) Find a power of 21 whose order is 8.
- (d) Use (a) and (c) to find a primitive element for F .

Lemma 2. *Let U be as above, and let x and y be elements of U , with orders s and t , respectively. Then U has an element whose order is $\text{LCM}[s, t]$.*

Proof. Write $s = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$ and $t = p_1^{f_1} \cdot \dots \cdot p_k^{f_k}$, where the p_i are distinct primes. We number the primes so that $e_1 \geq f_1, \dots, e_\ell \geq f_\ell$ and $e_{\ell+1} < f_{\ell+1}, \dots, e_k < f_k$. Let $a = p_1^{e_1} \cdot \dots \cdot p_\ell^{e_\ell}$ and $b = p_{\ell+1}^{f_{\ell+1}} \cdot \dots \cdot p_k^{f_k}$. (If $\ell = k$, that is, if $e_i \geq f_i$ for all i , then $t \mid s$, and we take $b = 1$.) Then $\text{LCM}[s, t] = ab$, and, moreover, a and b are relatively prime. Therefore, by Lemma 1, it will suffice to find elements whose orders are a and b . But this is easy: $x^{\frac{s}{a}}$ has order a , and $y^{\frac{t}{b}}$ has order b . \square

Proof of the Primitive Element Theorem. Let u be an element of U with largest possible order, say, m . I claim that, for every element v of U , the order q of v must divide m . For, if not, then $\text{LCM}[q, v]$ would be strictly greater than m . By Lemma 2, U would have an element of order $\text{LCM}[q, v]$, and this element would have order strictly larger than m , contradicting the choice of u . This shows that every element $v \in U$ satisfies the equation $v^m = 1$. Therefore the equation $x^m - 1$ has at least n distinct roots in F . Since a polynomial of degree m has at most m distinct roots, we see that $n \leq m$. However, $m \mid n$ by Fermat's theorem, and therefore $m = n$. Thus u is a primitive element. \square