Chapter 5: The Minimum Polynomial of an element of GF(q)

Chapter Contents.

Definition: *characteristic* p

The Minimum Polynomial m(x) of an element α in GF(q).

Definition: the *minimum polynomial* m(x) of some element α of GF(q)
Definition: *monic* polynomial: highest power has coefficient 1.
Fact 1: If p(α) = 0, p(x) is multiple of m(x)
Fact 2: List of basic m(x) properties
Fact 3: If monic f(x) is irreducible and has α as a root, then f(x) = m(x).

Primitive Polynomials and Period of m(x).

Definition: the *primitive polynomial* of α is m(x) of α when α is a primitive element of GF(q)
Definition: *period* of m(x) is minimum n such that m(x) divides $x^n - 1$
Fact 4: A primitive polynomial of GF(q) has period q-1
Fact 5: If period of m(x) of α is q-1, then α is a primitive element of GF(q)

Formula for the Minimum Polynomial m(x) of α.

Lemma 6: $f(x^p) = [f(x)]^p$ for any f(x) over GF(p)
Fact 6: m(x) for α is also m(x) for α^p.
Fact 7: m(x) for α is also m(x) for α^p, α^{pp} , α^{ppp}, ...
Definition: distinct α^p, α^{pp} , α^{ppp}, ... are the *conjugates* of α.
Definition: distinct α, α^p, α^{pp} , α^{ppp}, ... are the *conjugate set* of α.
Fact 8: If α is a primitive element, the conjugate set of α has m distinct elements, all of which are primitive elements
Fact 9: If α is not a primitive element, there may be fewer than m distinct elements in the conjugate set of α
Big Theorem 3: m(x) of α is the product of (x-a) factors, where a are all distinct members of conjugate set of α.
Fact 10: The degree of any primitive polynomial of $GF(p^m)$ is m.
Fact 11: The number of primitive polynomials for $GF(p^m)$ is equal to the number of distinct conjugate sets which contain primitive elements.
Examples: GF(8), GF(16)

On finding the primitive polynomials of $GF(p^m)$.

Fact 12: Reversing coefficients of a primitive polynomial gives another primitive polynomial.
References to tables of primitive polynomials.

Selecting f(x) for construction of $GF(p^m)$ = Polys[x,GF(p)]/ (f(x))

Fact 13: Not all monic irreducible polynomials over GF(p) are primitive polynomials.

Miscellaneous added facts:

Fact 14: Any monic, degree-m polynomial f(x) irreducible over GF(p) *is* the minimum polynomial of some element α of GF(p^m).

Fact 15: All roots of the conjugate set of α have the same order.

Corollary 15: All roots of any minimum polynomial m(x) have the same order. In particular, all roots of a primitive polynomial have order q-1.

Appendix 5.1: Description of the Conjugate Set of α

Chapter 5: The Minimum Polynomial of an element of GF(q)

In this chapter we continue to accumulate information about finite fields. As noted earlier, finite fields exist only for certain values of the order q. These values are of the form $q = p^m$ where p is a prime and m = 0,1,2,3..... The finite fields are denoted GF(q).

Definition: Some books refer to the prime number p as being the *characteristic* of GF(q).

The Minimum Polynomial m(x) of an element α in GF(q).

In Chapter 4 (Big Theorem 2) it was demonstrated that one could fully factor the polynomial $x^{q-1} - 1$ into a product of q-1 first degree factors, each of which vanishes at a non-zero element of GF(q):

$$x^{q-1} - 1 = (x - \mathbf{1}) \bullet (x - a_2) \bullet (x - a_3) \bullet (x - a_4) \bullet \ldots\ldots (x - a_{q-1})$$

We now keep sharply attuned to the distinction between coefficients in GF(p) and coefficients in GF(q). The polynomial $(x - a_4)$ has coefficients in GF(q), since a_4 is an element of GF(q). However, the polynomials (x - 1) or $(x^{q-1} - 1)$ have coefficients entirely in GF(p), which we know is a subfield of GF(q).

We pose this question: is it possible to take some set of the above factors that is less than the full set, and end up with some polynomial whose coefficients lie entirely in GF(p)? Clearly such a polynomial would have degree less than q-1 if it has less than all the factors.

There is one obvious such polynomial of degree q-2. You divide both sides by (x-1) to get:

$$1 + x + x^2 + \ldots + x^{q-2} = (x - a_2) \bullet (x - a_3) \bullet (x - a_4) \bullet \ldots\ldots (x - a_{q-1})$$

But is there a still *smaller* grouping that works? Ie, some *subset* of the above factors which produces a polynomial with coefficients in GF(p)? And assuming there is, we might ask: what is the smallest such polynomial? The one with the fewest factors.

One obvious way to find the smallest such polynomial is to make a huge list by multiplying factors together in all possible ways, then examine the resulting polynomials to see which ones, if any, have coefficients only in GF(p). We might call this the brute force method. We could then pick a particular element a_i of GF(q) and ask which of these polynomials with coefficients in GF(p) contain $(x - a_i)$ as a factor ? We could finally examine this smaller group and select the polynomial (or polynomials) having the lowest order, ie, having the least number of other factors. What you arrive at by this method would be called the *minimal polynomial of* a_i.

Definition: A "minimum polynomial for some element α of GF(q)" is the product of the smallest set of factors $(x - a_K)$ which contains the factor $(x - \alpha)$, *and* which has coefficients only in GF(p). Denote this minimum polynomial for α by the name m(x). Thus, α is a root of m(x), that is, $m(\alpha) = 0$.

Definition: If the coefficient of the highest power of a polynomial is 1, the polynomial is said to be monic. As defined above, any minimum polynomial m(x) is always monic, being a product of (x-a) factors.

For GF(p) with p>2, one can have coefficients other than 1 and 0. In this case, one can construct several superficially different polynomials which have the same roots, but they differ just by a scale factor. The monic requirement of m(x) then removes these superficial duplications. For example, 2x-2 is not really distinct from x-1 in GF(3), in terms of its roots.

Fact 1: If p(x) is a polynomial over GF(p) and $p(\alpha) = 0$, then p(x) is a multiple of m(x) of α.

Proof: Expand $p(x) = q(x)m(x) + r(x)$, where m(x) is a minimum polynomial of α, and where the degree of r(x) is less than that of m(x)-- this is the Division Algorithm of Chapter 3. If $p(\alpha) = 0$, then $r(\alpha) = 0$, since $m(\alpha) = 0$. But if $r(\alpha) = 0$, then m(x) must not be a minimal polynomial, since r(x) is a polynomial of lesser degree than m(x), and has α as a root. In other words, then r(x) must be the real minimum polynomial, not m(x). This contradicts the starting assumption, so we must have r(x) = 0. Thus, p(x) is a multiple of m(x).

Fact 2: The minimum polynomial m(x) for some element α of GF(q) has these properties:

(a) A unique m(x) exists for any given α
(b) $m(\alpha) = 0$
(c) m(x) is irreducible in GF(p)
(d) m(x) divides evenly into the polynomial $x^{q-1} - 1$

(a) Certainly we know that a minimum polynomial m(x) for any α must exist. If nothing smaller works out, we know that the polynomial shown above, $x^{q-1} - 1$, is the final candidate.

Suppose there were two mini\mum polynomials a(x) and b(x) for α. By definition, then $a(\alpha) = 0$ and $b(\alpha) = 0$. From Fact 0 applied twice, we conclude that a(x) is a multiple of b(x) and b(x) is a multiple of a(x). This can only mean that a(x) = b(x). Thus, the minimum polynomial is in fact unique.

(b) That $m(\alpha) = 0$ follows by definition since m(x) contains $(x-\alpha)$ as a factor.

(c) m(x) is irreducible in GF(p) since we said it has coefficients in GF(p), and m(x) had the lowest degree of all the candidates. If m(x) were reducible in GF(p), then we could write m(x) = a(x)b(x) where both a and b have coefficients in GF(p). That is what reducible means. Then, since $m(\alpha) = 0$, we know that either $a(\alpha) = 0$ or $b(\alpha) = 0$. In this case, we would take whichever one of these vanishes at α, and then that one would be our minimum polynomial. So really, by its very definition as being the $m(\alpha) = 0$ polynomial of lowest degree, we know that m(x) must be irreducible in GF(p).

(d) Since m(x) contains a subset of the factors than make up $x^{q-1} - 1$, it must divide evenly into $x^{q-1} - 1$. The quotient is then all the factors of $x^{q-1} - 1$ which are not contained in m(x).

Fact 3: If monic f(x) is irreducible over GF(p) and has some α of GF(q) as a root, then f(x) = m(x).

Proof: If $f(\alpha) = 0$, then $(x-\alpha)$ is a factor of f(x) -- this is Fact 7 of Chapter 4. If f(x) is irreducible over GF(p), then it has the lowest order possible and it has $(x-\alpha)$ as a factor. Since f(x) is monic, it has the right

overall constant scale factor. But this is the definition of m(x), and we know m(x) is unique. Thus, f(x) = m(x).

Primitive Polynomials and Period of m(x).

Definition: If α is a primitive element of GF(q), then the minimum polynomial m(x) of α is called a *primitive polynomial* of GF(q).

Corollary: If monic f(x) is irreducible over GF(p) and has some primitive element α of GF(q) as a root, then f(x) is a primitive polynomial of GF(q).

Proof: This is a restatement of Fact 3 for α = a primitive element of GF(q).

Definition: "period of m(x) " From Fact 2(d) we know that a minimal polynomial m(x) for any α in GF(q) divides $x^{q-1} - 1$. It may be possible that m(x) also divides $x^n - 1$ for some n that is smaller than q-1. The *smallest* such power n is called the *period* of m(x). Clearly, the period of m(x) is $n \leq q-1$. The reason for the name "period" will become clear later on. For the moment, it is just a word.

Fact 4: A primitive polynomial p(x) of GF(q) must have period q-1.

Proof: We know that p(x) is a minimal polynomial for some primitive element α of GF(q). We know by Fact 2(d) that p(x) divides $x^n - 1$ with n = q-1. Is there some smaller n?

Assume there exists some $n < q-1$ such that p(x) divides $x^n - 1$. Then $x^n - 1 = p(x)q(x)$ for some q(x). Since $p(\alpha) = 0$, we find $\alpha^n = 1$ for $n < q-1$. But by the definition of a primitive element, the order of α is q-1, and this means that n = q-1 is the smallest integer such that $\alpha^n = 1$. Thus we have a contradiction, so there is no $n < q-1$ that works. The smallest n that works is then q-1, so this is the period.

Fact 5: If the period of a some m(x) of α is q-1, then α must be a primitive element of GF(q), and m(x) is a primitive polynomial of GF(q).

Proof: If α is not primitive, then α has some order $n < q-1$. Thus, we can consider $(\alpha, n, \bullet)$, the cyclic subgroup generated by α. According to Fact 8 of Chapter 4, the n elements of this subgroup are the the n roots of $x^n - 1$, and we can factor as follows:

$$x^n - 1 = (x - a_1) \bullet (x - a_2) \bullet (x - a_3) \bullet \ldots (x - a_n)$$

where one of the a_i is our element α. Since $x^n - 1$ has coefficients in GF(p), it is a candidate for the minimum polynomial m(x) of α. The other possibility is that some subset of the factors shown here forms m(x). In either case, m(x) divides $x^n - 1$, so we have period $n < q-1$. But by hypothesis, the period of m(x) is supposed to be q-1. Thus, α must be a primitive element of GF(q), and by definition, m(x) is then a primitive polynomial of GF(q).

Formula for the Minimum Polynomial m(x) of α.

We would now like to develop an explicit formula for the minimum polynomial m(x) of α. As a very strong hint toward this end, we state and prove the following interesting fact:

Lemma 6: If f(x) is any polynomial over GF(p), then $f(x^p) = [\, f(x) \,]^p$.

Proof: Just write out both sides and make use of the GF(p) expansion formula given at the end of Chapter 2. The RHS becomes:

$$[f(x)]^p = [\, a + bx + cx^2 + \ldots \,]^p = (a)^p + (bx)^p + (cx^2)^p + \ldots = a^p + b^p(x^p) + c^p\,(x^p)^2 + \ldots$$

But we also know from the Chapter 2 list of facts that $a^p = a$ for any coefficient in GF(p), such as the coefficients a,b,c above. Thus we get

$$[f(x)]^p = a + b\,(x^p) + c\,(x^p)^2 + \ldots.$$

But this series is exactly $f(x^p)$, so our Lemma is proved.

Fact 6: If m(x) is the minimum polynomial for α, then m(x) is also the minimum polynomial for α^p .

Proof: From Lemma 6 we know that $m(x^p) = [\, m(x) \,]^p$. This means that $m(\alpha^p) = [m(\alpha)]^p = 0$, since m(x) is a minumum polynomial for α. Since m(x) is already known to be irreducible, and since $m(\alpha^p) = 0$, we have shown that m(x) is also a minimim polynomial for α^p. QED.

Fact 7: If m(x) is the minimal polynomial of α, then it is the minimal polynomial for *all* the elements in the following set of m elements,

$$\{\ \alpha,\ \alpha^p\ ,\ \alpha^{p^2}\ ,\ \alpha^{p^3}\ \ \ldots.\ \ \alpha^{p^{m-1}}\ \ \}\qquad\qquad \alpha^{p^m} = \alpha^q = \alpha\qquad\qquad \text{m elements}$$

Proof: Each element of this set is the previous element raised to the power p, so we just repeatedly apply our previous fact. For example $m[\ \alpha^{p^2}\ ] = m[\ (\alpha^p)^p\ ] = m[\ (\alpha^p)\ ] = m[\ \alpha] = 0$. We know from our list of facts at the end of Chapter 4 that $\alpha^{p^m} = \alpha^q = \alpha$. This is why the above list ends as shown. The next element would be a repeat of α, and the one after that would repeat α^p , and so on. There is no guarantee that the elements on the list as shown are all distinct, however. We shall return to this point later on.

Definition: The distinct members of the set of elements shown above is called the *conjugate set* of α, and the distinct elements other than α are called the *conjugates* of α. As already noted, each member of the above list is the previous member raised to the p power. Do not confuse this sequence with that of a cylic group which looks like $\{\ \alpha, \alpha^2\ , \alpha^3, \alpha^4,\ \ldots\}$ or maybe like $\{\ \alpha^p, \alpha^{2p}\ , \alpha^{3p}, \alpha^{4p},\ \ldots\}$. This conjugate list is a different beast.

Fact 8: If α is a primitive element of $GF(p^m)$, then

(a) the conjugate set of α contains the maximum number m of distinct elements

(b) all members of this conjugate set are primitive elements.

Proof: If α is a primitive element, then GF(q) contains all powers of α out to a maximum exponent of q-2. In the conjugate list above, the largest conjugate has power $p^{m-1} = p^m / p = q/p$. Thus, all the conjugate elements hit distinct elements of GF(q) as long as $q-2 \geq q/p$. This boils down to $p^{m-1}(p-1) \geq 2$. For any p>2 this is true for all m. For p=2, it is true for all m>1. We don't care about the case p=1 m=1 since this is GF(2) which we know all about. This field has no powers of α, is just has 0 and 1.

If α is a primitive, element, we know that α^p is also a primitive element since $GCD(p,p^m-1) = 1$. This is an application of Fact 12 of Chapter 4.

Fact 9: If α is *not* a primitive element, then it is possible that only the first k of the m conjugates of some element α are distinct, where k is very dependent on the field and on the field element selected. In this case, it turns out that we can write:

$$\{ \alpha, \alpha^p, \alpha^{p^2}, \alpha^{p^3} \ldots \alpha^{p^{k-1}} \} \qquad \alpha^{p^k} = \alpha \qquad \text{k conjugates} \qquad k \leq m$$

Proof: This is a slightly tricky proof which we defer to the Appendix of this chapter since it is a little long and takes us off the main line of presentation. It is included in the Appendix because we could not find it in any text and had to do it from scratch. What is happening here is that the conjugates are landing on the elements of a cyclic subgroup $\{ \alpha, \alpha^2, \alpha^3 \ldots \alpha^{n-1}\}$ where $\alpha^n = 1$. Since there might not be too many elements in such a subgroup, it seems reasonable that the m conjugates in the original list might hit the same elements more than once. What is not obvious is that the first repeated element is α, as implied above. This turns out to be true, and moreover, as higher and higher powers are applied, the same elements in the subgroup are hit in the same order that they were first hit, and this hitting sequence cycles over and over. Furthermore, certain members of the cyclic subgroup may never be hit.

Big Theorem 3: The minimum polynomial of an element α of GF(q) may be written as follows:

$$m(x) = (x-\alpha) \bullet (x - \alpha^p) \bullet (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots \ldots (x - \alpha^{p^{k-1}}) \qquad \alpha^{p^k} = \alpha$$

In other words,the claim is that the minimum polynomial m(x) is the product of linear factors of the form $(x-a_i)$, where the a_i are all the distinct elements of the conjugate set of α. The order of this polynomial is then equal to the number of distinct elements in the conjugate set of α, which we call k, and we know that $k \leq m$. One obvious way to construct m(x) is to compute up the factors one at a time as shown above until the repeat value k is reached.

Proof: The proof is simple and fascinating. First of all, we already know that m(x) must have at least all the factors shown above. It can have no smaller number of factors. This is because it needs all these factors to vanish at all the conjugate elements, and we showed above that m(x) must vanish at all members of the conjugate set of α. If we can show that the coefficients of the m(x) given above are all in GF(p), then we are done.

Here is the trick. Write the pth power of m(x) in two different ways. First, compute $[m(x)]^p$ by raising each linear factor to power p. Then apply the theorem that $(a+b)^p = a^p + b^p$. Here is what happens to one factor:

$$(x - \alpha^{p^2})^p = (x^p - \alpha^{p^3})$$

It has become the next factor to the right, and x is replaced with x^p. So what happens to the final factor on the right? It becomes the one on the far left, with x replaced by x^p. We have thus shown that:

$$[m(x)]^p = m(x^p) = \sum_i a_i (x^p)^i$$

In the last step we just expanded polynomial m(x) in terms of its coefficients. On the other hand, we could have *started* with this coefficient expansion of m(x) and raised *it* to the power p, and then used the generalized expansion theorem (see end of Chapter 4) to get:

$$[m(x)]^p = (\sum_i a_i (x)^i)^p = \sum_i (a_i)^p (x^p)^i$$

For these polynomials to be equal, the coefficients must all match, we we get that $(a_i)^p = a_i$. According to Fact 16 of Chapter 4, this means all the a_i are elements of GF(p). Thus, m(x) as shown has coefficients in GF(p) and has the fewest number of factors possible, so it is in fact the minimum polynomial of α.

Fact 10: The degree of any primitive polynomial of $GF(p^m)$ is m.

Proof: A primitive polynomial is a minimum polynomial m(x) for some primitive element α. According to Fact 8 above, the conjugate set of α has m distinct elements if α is primitive. Then according to Big Theorem 3, we see that there is one factor (x - a) for each distinct element in the conjugate set of α, so there are m factors. Thus, the degree of m(x) is m.

Fact 11: The number of primitive polynomials for GF(p^m) is equal to the number of distinct conjugate sets which contain primitive elements.

Proof: According to Big Theorem 3, the number of distinct minimal polynomials equals the number of distinct conjugate sets. Suppose there are N such sets, and suppose M of these contain primitive elements. Then there are M unique primitive polynomials.

For $q = p^m$, we know that each set of conjugates has at most m distinct elements. If a conjugate set contains a primitive element, then all m members of the set must be distinct.

Example: Let us enumerate GF($2^3 = 8$),

$\{ 0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6 \}$ $\alpha^7 = 1$

Which elements are primitive elements besides α? Fact 12 of Chapter 4 tells us that a power α^k is a primitive element if GCD(k,7) = 1. So k = 1,2,3,4,5,6 all define primitive elements. Next, let's construct the conjugate sets. Each contains at most 3 elements:

$\{ \alpha, \alpha^2, \alpha^4\}, \{ \alpha^3, \alpha^6, \alpha^5\}, \{1\}$

So N = 3, but only M=2 of these conjugate sets contain primitive elements, so there are two distinct primitive polynomials for GF(8). Here they are:

$m(x; \alpha) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$
$m(x;\alpha^3) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^5)$

Example: Let us enumerate GF($2^4 = 16$),

$\{ 0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}$ $\alpha^{15} = 1$

Which elements are primitive elements besides α? Fact 12 of Chapter 4 tells us that a power α^k is a primitive element if GCD(k,15) = 1. So k = 1, 2, 4, 7, 8, 11, 13, 14 all define primitive elements. Next, let's construct the conjugate sets:

$\{ \alpha, \alpha^2, \alpha^4, \alpha^8 \}, \{ \alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}, \{ \alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}, \{ \alpha^5, \alpha^{10} \}, \{1\}$

So N = 5, but only M=2 of these conjugate sets contain primitive elements, so there are two distinct primitive polynomials for GF(16).

Notice in the above two examples that if one member of a conjugate set is a primitive element, then all members are, as claimed in Fact 8(b).

On finding the primitive polynomials of GF(p^m).

We know that these polynomials f(x) will be of degree m (Fact 10), are irreducible over GF(p) (Definition), and they must have period $p^m - 1$ (Fact 4).

The fact that $f(\alpha) = 0$ for some primitive element in GF(q) is true, but is not very useful toward constructing the polynomials. For example, in GF(8) we can try to construct p(x) for primitive element α according to Big Theorem 3,

$$p(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 - x^2 [\ \alpha + \alpha^2 + \alpha^4\ ] - x[\ \alpha^3 + \alpha^5 + \alpha^6\ ] + 1$$

But we cannot do much else without knowledge of the addition table in the powers-of-α basis. If we have this table, then we can do the sums shown and get a result. However, to get the tables in the first place requires the selection of some irreducible F(x) of degree m, such that

$$GF(p^m) = Polys[x, GF(p)] / (F(x))$$

Note that F(x) does not have to be a primitive polynomial, nor does it have to even be a minimum polynomial. It need only be irreducible in GF(p). Such a polynomial can easily be found, and the + and • tables constructed. Then one must identify a primitive element α. This seems like a lot of work just to have a + table to determine the primitive polynomials.

Probably a better way is trial and error. In the above p(x) case, each [] coefficient is either 1 or 0, so there are only 4 polynomials to try. Here they are:

$x^3 + x^2 + x + 1$	$= x^2 (x + 1) + (x+1)$ = reducible
$x^3 + x^2 + 1$	
$x^3 + x + 1$	
$x^3 + 1$	$= x^3 - 1$ = reducible

Since we know there are two primitive polynomials for GF(8), and we have only two candidates in the list, they must be the ones. We did not even have to check that the period of each is 7, we know it must be true. Notice that we always have a + 1 added on, otherwise the polynomial would be reducible since it would have a factor x.

For GF(16) there are more possibilities to worry about:

$x^4 + x^3 + x^2 + x + 1$	n = 5
$x^4 + x^3 + x^2 + 1$	
$x^4 + x^3 + x + 1$	$= (x^3+1)(x+1)$
$x^4 + x^2 + x + 1$	
$x^4 + x^3 + 1$	°
$x^4 + x + 1$	•
$x^4 + x^2 + 1$	
$x^4 + 1$	= reducible

Now there are 6 candidates left, they all look irreducible, so now one would have to apply the period test to each. Which ones divide into $x^n - 1$ for n less than 15? The first one we can see divides into $x^5 - 1$, so we throw it out. The others are less obvious. It would appear that tedious long divisions are necessary to eliminate 3 out of the remaining 5 polynomials.

The one with a dot • is indicated in texts as a primitive polynomial, so one suspects "by symmetry" that the one above it is the other one. That symmetry rule is the following:

Fact 12: If f(x) is a primitive polynomial, then so is f*(x) defined by reversing the coefficients. Thus, in the above list, if • is primitive, so is ° . It is easy to show that $f^*(x) = x^m f(1/x)$.

Proof: See Peterson and Weldon, Problem 6.7. You basically need to show that f*(x) is irreducible and has the same period as f(x).

Observation: There are of course automated procedures to scan all polynomials f(x) of a given degree m and find which ones are irreducible and which of those are primitive. This last step requires checking that the *period* of f(x) is q-1, where $q = p^k$. This means you have to try dividing f(x) into $x^n - 1$ and make sure it does not go for any power n less than q-1. For a high order, there are a *lot* of polynomials to try. For example, if $q=2^{50}$, you have $2^{50} = 10^{15}$ candidate polynomials to test. Obviously, people who make the tables make use of some heuristic methods.

Tables of irreducible polynomials for any order ≤ 34 are given in Peterson & Weldon, Appendix C, and those which are primitive are noted. More extensive tables appear in Lidi and Niederreiter, *Finite Fields*. A list of one primitive polynomial for each n in the range (1,100) is included as an appendix in our Scrambler notes Chapter 2. See E.J. Watson, **Math. Comp.** 16, 368-369 (1962).

Selecting f(x) for construction of GF(p^m) = Polys[x,GF(p)]/ (f(x))

In Chapter 4 we were able to construct a representation of GF(p^m) by starting with any irreducible polynomial of degree m, $q = p^m$. We made the identification:

$$GF(p^m) = Polys[x,GF(p)] / (f(x))$$

As our GF(16) example above shows, even when p=2, there are typically many candidates for f(x), all of which give an equivalent representation of GF(p^m). Moreover, for p>2, every candidate has p-2 shadow candidates which are just scale factor multiples of f(x).

By our definition, a primitive polynomial is monic and so the shadow candidates are eliminated. Since a primitive polynomial of degree m is irreducible, it can serve as an f(x) in the construction of GF(p^m) as the extension field over GF(p). However, it is not necessary to use a primitive polynomial to accomplish the construction. As we shall see in the next chapter, there is a great advantage to using a primitive polynomial for this purpose. As a reminder, then:

Fact 13: Not all monic irreducible polynomials over GF(p) are primitive polynomials.

The following two facts are a bit out of order in their appearance here, but we felt they should be stated somewhere.

Fact 14: Any monic, degree-m polynomial f(x) irreducible over GF(p) *is* the minimum polynomial of some element α of GF(p^m).

Proof: In the next chapter we will show that $\alpha = \{x\}$ is a root of any polynomial f(x), and {x} is an element of any GF(q). Thus, one can always find *a* Galois root of f(x). Fact 14 then follows from -- and is a stronger version of -- Fact 3.

Fact 15: All roots of the conjugate set of α have the same order.

Proof: Let α have order n. From (Chapter 4) Fact 6 we know that order(α^p) = n/GCD(p,n). But from Chapter 4 Fact 1 , n must divide $p^m - 1$, so write $p^m - 1 = nk$. Now consider

$$GCD(p,n) = GCD(p, [p^m - 1]/k)$$

Since p is prime, this thing is 1 unless the second argument is a multiple of p. Assume that $[p^m - 1]/k$ is a multiple of p, so then $p^m - 1 = kNp = Mp$. But this then implies that $(p^m - 1)/p = p^{m-1} - 1/p = M$. But this is impossible since 1/p is not an integer (ignoring p=1), so $[p^m - 1]/k$ cannot be a multiple of p, and thus GCD(p,$[p^m - 1]/k$) = 1. We conclude then that order(α^p) =order(α) = n. Continuing in this way, we show that all elements of the conjugate set of α have the same order.

Corollary 15: All roots of any minimum polynomial m(x) have the same order. In particular, all roots of a primitive polynomial have order q-1.

Appendix 5.1: Facts about the Conjugate set of α

Here we wish to examine what happens as one keeps raising the conjugate exponent in the series

$\{ \alpha, \alpha^p, \alpha^{p^2}, \alpha^{p^3} .... \alpha^{p^{m-1}} \}$ conjugate sequence

It is useful to think for the moment of m being very large, so there are many terms to worry about.

We know that α is a member of some cyclic subgroup under • of some order n-1. Thus, we write

$\{1, \alpha, \alpha^2, \alpha^3, ... \alpha^{n-2} \}$ the landing zone $\alpha^{n-1} = 1\ \alpha^n = \alpha$

Definition: Let's call n the *repeat index* of this cyclic subgroup of order n-1.

Imagine that this set is relatively small, while the set of conjugates is relatively large. As we step sequentially through the conjugates, each one maps onto (lands on, equals) some element in this little cyclic group. This is entirely controlled by the fact that $\alpha^n = \alpha$. In fact, here is how the mapping works:

exponent of α in the landing zone = $\text{Rem}(p^k/n) = r_k$

We are just taking the conjugate's exponent and figuring it modulo n. As the conjugate sequence start off with k = 0,1,2... we hit the elements $(\alpha)^{r_k}$ in the cyclic group. We know that $r_0 = 1$, and $r_1 = p$ if $p < n$. In any event, we land on a certain sequence of elements in the cyclic group, not necessarily in any reasonable order. The conjugate sequence is traversed in order, but the hits in the landing zone might be in a strange order, and various elements might not be hit because their exponent r_k might never show up.

Notice by the way that all the r_k would vanish if n were a power of p. Thus we show that:

Fact: Order n is not a power of p.

Proof: The repeat index n of a cyclic group must evenly divide the order $q - 1 = p^m - 1$ of { GF(q) -0}. But any power of p does not divide this number evenly. In fact, the remainder is always 1.

Let us now assume there is some minimum $k = k_0 > 0$ such that $\text{Rem}(p^{k_0}/n) = 1$. For example, if n = 5 and p = 2, we get $k_0 = 4$. If there is no k_0 that is less than m (the max number of conjugates), then nothing repeats within the limited set of conjugates shown above. So assume k_0 does exist.

This means that the conjugate labelled by k_0 will land on α. Since k_0 is assumed to be the smallest solution to the above condition, this is the first conjugate to hit α after the first hit with k = 0.

Fact: We now claim this to be true: $\text{Rem}[\ \frac{p^{(k_0+ s)}}{n}\ ] = r_s$, the same r_s numbers given above.

Proof: Apply Little Lemma 1 of Chapter 1 to show that:

$$\text{Rem}\left[\frac{p^{(k_0+s)}}{n}\right] = \text{Rem}\left[\frac{p^s \,\text{Rem}[p^{k_0}/n]}{n}\right] = \text{Rem}\left[\frac{p^s\, 1}{n}\right] = r_s$$

So we encounter a repeat of the α hit when $k = k_0$, then as s counts up s = 0,1,2... we run through the same values r_s as when we started, so we repeat the hit sequence on the elements of the cyclic group in the same order that occurred the first time (whatever strange order this might have been).

Fact: $\text{Rem}\left[\frac{p^{(Nk_0+s)}}{n}\right] = r_s$, the same r_s numbers given above, for N = 0,1,2...

Proof: This is the same as the last fact, but we have added N. We prove this by induction. Assume it is true for some N (we know N=0 or N=1 works), and show true for N+1. Our proof makes two uses of Little Lemma 1 of Chapter 1:

$$\text{Rem}\left[\frac{p^{((N+1)k_0+s)}}{n}\right] = \text{Rem}\left[\frac{p^{k_0}\,\text{Rem}[p^{(Nk_0+s)}/n]}{n}\right] = \text{Rem}\left[\frac{p^{k_0}\, r_s}{n}\right] =$$

$$= \text{Rem}\left[\frac{r_s\,\text{Rem}[p^{k_0}/n]}{n}\right] = \text{Rem}(r_s\, 1/n) = r_s$$

This fact then shows that, as conjugate index k keeps increasing, each time we hit a multiple of k_0, and then step through the next conjugates with s = 0,1,2,3..., we again hit the the elements of the cyclic group in the same order as the original time.

So we cycle again and again through the subset of the cyclic group elements that gets hit. After the first time through, the first "repeat" is a hit on α which occurs when $k = k_0$.

So the question of whether all m conjugates are distinct in the original set boils down to the question of whether there exists a k_0 such that $\text{Rem}(p^{k_0}/n) = 1$, where k_0 is less than m. This in turn depends on the order n of the cyclic subgroup which contains element α. This suggests that all elements of a given cyclic subgroup will have the same number of distinct conjugates.

Finally, if n = q-1 as for a primitive element, there is clearly no k_0 that works:

$$\text{cannot find } k_0 < m \text{ such that } \text{Rem}\left[\frac{p^{k_0}}{p^m - 1}\right] = 1$$

and in this case there are no repeats, and we get the full set of m conjugates.