Are the period of h(x) and the order of one of its α's related? PhL 6.29.13

This doc has two items to be added to Galois. The first is a new proof of (5.35) which I have already installed. The second is my theorem that order = period, and I now need to ponder where that should go. I did so, and it too is now installed as Chapter 5 (k). Everything useful is now extracted from this doc!

All items in this doc have been added to Galois doc.

Where to put order = period? It involves conjugate sets and min polys so Chap 5 on min polys seems a good place. My use of "period" in Galois was merely as a test one could use to identify a primitive polynomial. I never really USED it for anything significant and thus did not care much about it.

I guess it can really only go as a new section at the end and then it would be (k).

Is there a connection between the order of α and the period of h(x) whose first factor is that α ? In (2.3.11) they seem to be equal. I make no connection between these two integers in either document.

The **period** of h(x) is the smallest n which appears here: $g(x) = (x^n-1)/h(x)$

The **order** of α is the smallest n such that $\alpha^n = 1$.

The **element α** is what appears in this formula for a minimum polynomial

$$m(x) = (x - \alpha) \bullet (x - \alpha^p) \bullet (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots \ldots (x - \alpha^{p^{k-1}}) \qquad \alpha^{p^k} = \alpha \qquad k \le m \qquad (5.17)$$

Here I am not assuming h(x) is a primitive polynomial. Notice that if $\alpha^n = 1$ then this is true for all elements of the conjugate set of α, but it is not clear whether n would be the smallest integer for which this would be true for some given element. Now perhaps write

$$g(x)h(x) = (x^n - 1)$$

Here n is the smallest integer for which we can make this equation be true (the period). Certainly then

$$g(\alpha)h(\alpha) = (\alpha^n - 1)$$

Since h(α) = 0 for any conjugate set α, we know that $\alpha^n = 1$ for such an α. But could there be some smaller value, call it m, for which this is true? Could the period be smaller than the order?

In GA I introduce the **period** in (5.9).
In GA I introduce the **order** in (4.17) and (4.18). The order of α is the order of the cyclic subgroup generated by α, and this agrees with order being smallest integer n such that $\alpha^n = 1$.

In Fact 6 I come up with a formula for order:

Fact 6: If β is any element of (α,n,•), then the **order** of β divides n, the order of α. More specifically, we claim that [order of β] = n/GCD(k,n) where $\beta = \alpha^k$. (4.21)

Note that implicitly through (α,n,•) the above says that n is the order of α. So if I know the order of one element, I can compute that of others and it can be different. If α is a primitive element, I know that it has order q-1.

Can I find a non-primitive h(x) which has order ≠ period?

Let's go back to the min poly formula

$$h(x) = (x - \alpha) \bullet (x - \alpha^p) \bullet (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots \ldots (x - \alpha^{p^{k-1}}) \qquad \alpha^{p^k} = \alpha \qquad k \le m \qquad (5.17)$$

and let's assume that n is the period of h(x) so that $g(x) = (x^n-1)/h(x)$ has the smallest n.

Question: Do all elements of the conjugate group of α have the same order?

I spent time in the blue below which I will later delete, and found that the answer is YES.

The general element is α^{p^i} for i = 0 to k-1. Assume that α has order n. Then from the formula above we know

$$n' \equiv \text{ order of } \alpha^{p^i} = n/\text{GCD}(p^i,n)$$

Example: Suppose n = 4, p = 2 and i = 2. Then n' = 4/GCD(4,4) = 4/4 = 1 !!! So then n' ≠ n.

Can I find an explicit example? Where have I stated the order of any α for some actual example?

OK, let's work on all the min polys of GF(2^4) which I at least know.

$$p_1(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) = x^4 + x + 1$$
$$p_7(x) = (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11}) = x^4 + x^3 + 1$$
$$m_3(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = x^4 + x^3 + x^2 + x + 1$$
$$m_5(x) = (x - \alpha^5)(x - \alpha^{10}) = x^2 + x + 1 \qquad \text{GA (6.21)}$$

How can I compute the period of each h(x) and the order of α ? I think the period is easy. I just try 15, 5 and 3 and find the smallest of these three integers for which Rem = 0.

$x^4 + x + 1$	period = 15	
$x^4 + x^3 + 1$	period = 15	
$x^4 + x^3 + x^2 + x + 1$	period = 5	3 does not work
$x^2 + x + 1$	period = 3	5 does not work

Now how do I compute the order of some α involved in the above? What is α in the above list?? I know it is some primitive element due to the fact that p_1 is a primitive polynomial. I know then a whole set of elements which are primitive, all those appearing in p_1 and p_7. There are 8 of these including α. All of these 8 guys have order 15 because they are primitive. They are generators of GF(16) - 0. But what are the orders of all the other 7 elements? Since α has order 15, we can say

n' = order of α^k = 15/GCD(k,15)

```
for k from 1 to 15 do
   np :=15/gcd(k,15):
   print(k, np)
od:
```

1, 15
2, 15
3, 5
4, 15
5, 3
6, 5
7, 15
8, 15
9, 5
10, 3
11, 15
12, 5
13, 15
14, 15
15, 1

I confirm that the prim poly elements all register 15 for order. But then

$m_3(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)$

order $\alpha^3 = 5$
order $\alpha^6 = 5$
order $\alpha^{12} = 5$
order $\alpha^9 = 5$

Hmmm. Next we have

$m_5(x) = (x - \alpha^5)(x - \alpha^{10})$

order $\alpha^5 = 3$
order $\alpha^{10} = 3$

This is not what I expected. I thought I showed that in a min poly the orders of the factors could be different. Let's go back to my formula

$$n' \equiv \text{ order of } \alpha^{p^i} = n/GCD(p^i,n)$$

Now if α is a primitive element, then we know order $\alpha = p^m - 1 = n$ and then we are saying

$$n' \equiv \text{ order of } \alpha^{p^i} = (p^m - 1)/GCD(p^i, p^m - 1)$$

If it is true (as seems likely) that $GCD(p^i, p^m - 1) = 1$ for i = 1..k-1, then all conjugate elements have the same order as I found in my example above. In this case we consider

$$GCD(2^i, 2^4 - 1) = GCD(2^i, 15)$$

Since the first term is even and the second is odd, the result is always 1. The only chance is if 2^i were an even multiple of 15, but i does not go far enough for that to be true. I think I studied exactly this problem somewhere in Galois! It is not in an appendix. It was some pure math fact that I needed somewhere. I was showing two things could not be equal. How do I search for such an artifact with no handle? I found it by scanning through, see (9.27)

Lemma 1: There is no integer n such that, given m and p>1, $(p^m-1)/(p-1) = p^n-1$. (9.27)

So although similar, this is not quite related. So lets roll our own.

Theorem (?): $GCD(p^i, p^m - 1) = 1$ for p prime and i = 1,2....m

Assume there exists integer N > 1 such that

$$GCD(p^i, p^m - 1) = N$$

Then there exist integers I and J such that

$p^i/N = I$ $\quad$ $p^i = NI$

$(p^m - 1)/N = J$ $\quad$ $p^m - 1 = NJ$ $\quad$ $(p^m - 1)/p^i = J/I$

If p is prime, then p is odd. Then p^i is odd since odd*odd = odd. And $p^m - 1$ is even. then

odd = NI

even = NJ

If N were even, then I is odd and J could be even or odd. going nowwhere.

How about Bezout.

• **Euclidean Algorithm and Bezout's Identity**. The Euclidean Algorithm is a set of instructions one can use to find $d = GCD(n_1,n_2)$ for any integers n_1 and n_2. Bezout's Identity says that this common divisor d can be expressed in the following manner, where a and b are integers,

$$d = a\, n_1 - b\, n_2 \qquad \{\text{replace b with -b to get the usual form of this identity}\} \qquad (1.43)$$

You are given n_1 and n_2, and regardless of whether you have computed $d = GCD(n_1, n_2)$, you know that there exist two integers a and b (either could be negative) such that $d = a\, n_1 - b\, n_2$.

OK, set $n_1 = p^i$ and $n_2 = p^m - 1$. Then integers a and b exist such that

$$N = a\,p^i - b\,(p^m - 1)$$

I am learning nothing new here. How about a counter example search. Maple seems to say that the result is true no matter what integer p is, does not have to be prime. Start over:

Theorem (?): $\mathrm{GCD}(p^i, p^m - 1) = 1$ for p = integer and m = integer range i = 1 to m

$p^i/N = I$ $\quad p^i = NI$

$(p^m - 1)/N = J$ $\quad p^m - 1 = NJ$ $\quad (p^m - 1)/p^i = J/I$

We can write $p^m = p^i\,p^{m-i}$ so then

$$p^m - 1 = NJ$$
$$p^i\,p^{m-i} - 1 = NJ$$
$$NI\,p^{m-i} - 1 = NJ$$

This last line then says

$$N(I\,p^{m-i} - J) = 1$$

$$I\,p^{m-i} - J = 1/N$$

But if N > 1, the left side is an integer and the right side is a fraction QED!!!

So if nothing else, I have come up with a new Fact. But I see this is just Fact 15 of (5.35), I have already been up this little canyon. But maybe I have here a better proof

Here is my new proof to install into Galois

****

Equation (5.3) already exists and states this fact. Here I just have a better proof with a separate Lemma and a nice Maple verification. Here is the previous proof:

Fact 15:

(a) All roots (elements) of the conjugate set of α have the same order.

(b) If α is primitive, that order is q-1 and all elements are then primitive. (5.35)

Proof: The order n of α is defined in (4.17) item (e) as the order of the cyclic group generated by α, and (4.16) states that this order must divide evenly into q-1 which is the order of {GF(q)-0}. From (4.21) we know that order(α^p) = n/GCD(p,n). Since n must divide $p^m - 1$, we write $p^m - 1 = nk$. Now consider

$$\text{GCD}(p,n) = \text{GCD}(p, [p^m - 1]/k) .$$

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 N 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 $\text{GCD}(p,[p^m - 1]/k) = 1$. We conclude then that $\text{order}(\alpha^p) = \text{order}(\alpha) = n$. Continuing in this way, we show that all elements of the conjugate set of α have the same order. Part (b) is a trivial corollary.

I just like the new proof better and it does not need p = prime. I just installed it, **DONE**.

Fact 15: (a) All elements of a conjugate set have the same order.
(b) If α is primitive then all elements of the conjugate set of α are primitive (order q-1). (5.35)

Proof: (b) If α is primitive, it has order q-1 by definition. From part (a), all other elements of the conjugate set have order q-1. They are thus all primitive elements of GF(q).

(a) According to (5.17), the elements of a conjugate set of α all have the form α^{p^i} where i ranges from 0 to some $k \le m$. From (4.17) (**ℓ**) we know the order of α must divide p^m-1 so write $[\text{order of } \alpha] \equiv n = (p^m-1)/K$ where K is an integer. According to (4.21),

$$[\text{order of } \alpha^{p^i}] = n / \text{GCD}(p^i, n) = [\text{order of } \alpha] / \text{GCD}(p^i, (p^m-1)/K) .$$

If we can show that $\text{GCD}(p^i, (p^m-1)/K) = 1$, then our Fact is proven since $[\text{order of } \alpha^{p^i}] = [\text{order of } \alpha]$.

Lemma: Show that $\text{GCD}(p^i, (p^m-1)/K) = 1$ for i = 0,1....m (note that $m \ge i$) . (5.35a)

Assume that $\text{GCD}(p^i, (p^m-1)/K) = N > 1$. Then we can write

$$p^i/N = I \quad \Rightarrow \quad p^i = NI$$
$$[(p^m-1)/K]/N = J \quad \Rightarrow \quad (p^m-1) = NJK$$

where I and J are integers. Write $p^m = p^i\, p^{m-i}$ where $m-i \ge 0$ so then the last equation above becomes

$$(p^i\, p^{m-i} - 1) = NJK .$$

But $p^i = NI$ so we have

$$(NI\, p^{m-i} - 1) = NJK$$
$$N(I\, p^{m-i} - JK) = 1$$
$$(I\, p^{m-i} - JK) = 1/N .$$

Since the left side is an integer and the right side is a fraction, we have a contradiction, so N = 1. Notice that the fact that p = prime was not necessary in this Lemma proof.

It never hurts to test a proof in Maple. Here we search through all $GF(p^m)$ for a range of p and m to see if we encounter any cases of $\text{GCD}(p^i, (p^m-1)/K) \ne 1$. The commented-out print line is used for debug.

```
> with(numtheory): pmax := 10: mmax := 10: found := 0:
> for p from 2 to pmax do
    for m from 1 to mmax do
      for K in divisors(p^m-1) do
        for i from 0 to m do
          g := gcd(p^i,(p^m-1)/K);
          if g <> 1 then print(p,m,p^m-1,K,i,g); found := 1 fi;
          # print("p,m,p^m-1,K,i,g = ", p,m,p^m-1,K,i,g);
        od;
      od;
    od;
  od;
  if found = 0 then print( "no cases found") fi;
                                  "no cases found"
```

****

I think the following fact is true and I will try to prove it. This is a first shot, better one below.

Fact: The order of any of the GF(q) elements which form a minimum polynomial m(x) is equal to the period of h(x).

I have found this to be true in one example and I suspect it is true in general. We write

$$m(x) = (x - \alpha) \bullet (x - \alpha^{p}) \bullet (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots \ldots (x - \alpha^{p^{k-1}}) \qquad \alpha^{p^k} = \alpha \qquad k \le m \qquad (5.17)$$

Here α is not in general a primitive element, so it just has some order N which is a divisor of q-1.

Let N be the order of α:	$\alpha^N = 1$	N is smallest so true N must divide q-1 evenly
Let n be the period of m(x)	$m(x)g(x) = (x^n-1)$ $\Rightarrow \alpha^n = 1$ doing the {x} trick n must divide q-1 evenly	n is smallest integer so true

So at least period n is a *candidate* for order N, but there could be some smaller N.

So assume the order of α is some N < n. We seek a contradiction. I do have this extra fact

$$N = [\text{order of } \alpha] = s/GCD(k,s) \text{ where } \alpha = \beta^k \qquad s = \text{order of } \beta \qquad (4.21)$$

In this last line, I can regard β as a primitive element if I want, and there will be some k such that $\alpha = \beta^k$. In this case, I know s = q-1 so we have

$$N = [\text{order of } \alpha] = (q-1)/GCD(k,q-1) \quad \text{where } \alpha = \beta^k \quad \beta = \text{primitive element of GF(q)}$$

$m(x)g(x) = (x^n-1)$
$k \quad n-k \qquad n$

How exactly does one compute the period of m(x) ? Is the only way to do trial and error division to see if there is a remainder for each of the divisors of q-1? This has been my impression.

Let's examine some known fields. For GF(32) we have q-1 = 31 so it has no divisors so we can learn nothing from this case. For GF(16) there are only 4 min polys and order = period for all of them. For GF(8) all the polys are prims. So I have no ready-made examples to ponder.

Go back again to what we know already:

$g(x) = (x^n-1)/m(x)$ n is smallest integer so no remainder

$g(x)m(x) = (x^n-1)$

$g(\{x\})m(\{x\}) = (\{x\}^n - 1)$

But what do I know about {x}? It is hard to find this in GA, it is all spread out.

Locating {x} information in GA
Notation first introduced above (3.14)
More on this above (6.2)
Here is (6.5):

Fact 1: $f(\alpha) = 0$ for $\alpha = \{x\}$. { α *may* or may *not* be a primitive element of GF(q) } (6.5)

Here f(x) is used in R/I think for GF(q). So {f(x)} = 0 since no remainder on f(x) division. So f({x}) = 0. So OK, I know that I am using my m(x) to create GF(q) so I do know that m({x}) = 0.

I can then continue the above

$g(x)m(x) = (x^n-1)$ where no smaller n works

$g(\{x\})m(\{x\}) = (\{x\}^n - 1)$

$g(\{x\})\ 0 = (\{x\}^n - 1)$

$\{x\}^n = 1$

Can this be run either way? No!

{ f(x) } = { g(x) } does not imply f(x) = g(x)

It does imply $\quad\quad$ Rem(f(x)/m(x)) = Rem (g(x)/m(x))

$f(x) = q_f(x)m(x) + r_f(x)$
$g(x) = q_g(x)m(x) + r_g(x)$

I need either a proof or a counterexample. I cannot stop until one or the other is found. A web scan turned up the P&W min poly list which I am now studying on web though I have it as well. I quote

> The exponent to which a polynomial belongs can be found as follows: If a is a primitive element of GF(2^m), then the order e of a^j is
>
> $$e = (2^m-1)/GCD(2^m-1, j)$$
>
> and e is also the exponent to which the minimum function of a^j belongs. Thus, for example, in GF(2^{10}), a^{55} has order 93, since
>
> $$93 = 1023/GCD(1023, 55) = 1023/11$$
>
> Thus the polynomial (3453) belongs to 93.

The first equation says that e is the *order* of a^j . Now I think that

"h(x) has *period* n" $\quad\quad\leftrightarrow\quad\quad$ "n is the *exponent* to which min function h(x) belongs"

so in his example, the GCD formula shows that in GF(2^{10}), if α is a prim element, then α^{55} has order 93 and this should be the period of h(x) which is the min poly of α^{55}. How does he know that (3453) in octal is such a min poly? Well, here is his table for GF(10)

DEGREE	10	1	2011E	3	2017B	5	2415E	7	3771G	9	2257B
11	2065A	13	2157F	15	2653B	17	3515G	19	2773F	21	3753D
23	2033F	25	2443F	27	3573D	29	2461E	31	3043D	33	0075C
35	3023H	37	3543F	39	21078	41	2745E	43	2431E	45	3061C
47	3177H	49	3525G	51	2547B	53	2617F	55	3453D	57	3121C
59	3471G	69	2701A	71	3323H	73	3507H	75	2437B	77	2413B
83	3623H	85	2707E	87	2311A	89	2327F	91	3265G	93	3777D
99	0067	101	2055E	103	3575G	105	3607C	107	3171G	109	2047F
147	2355A	149	3025G	155	2251A	165	0051	171	3315C	173	3337H
179	3211G	341	0007								

and you see 3453D next to 55, which means it is a min poly of α^{55}.

Next we have this

> 1. The residues of 1, X, X^2, X^4, ... , X^{2m-1} are formed modulo f(X).

What is a residue? I have to go get the book and search. I only refer to "residue class ring", never residue by itself. WP also use "residue class" exclusively, never "residue" along until page 209 where we get this

If the roots are given as powers of a single element α of order e, that

.....

the integers e and u_i as follows. By Theorem 6.26, all the roots of $m_i(X)$ are contained in the sequence $\alpha^{u_i}, \alpha^{u_i q}, \alpha^{u_i q^2}, \alpha^{u_i q^3}, \ldots$, and hence all the roots are all the distinct elements in this sequence. The exponents, then, are the distinct residues modulo e of $u_i, u_i q, u_i q^2, u_i q^3, \ldots$, and the number of distinct residues is the degree r_i of $m_i(X)$. It is quite possible

The roots of m(x) are the conjugate set of α^{ui} in his example, like my statement

exponents = { s, sp, sp^2, sp^3, ... sp^{k-1} }. and { α^s, α^{sp}, α^{sp^2}, α^{sp^3}, ... $\alpha^{sp^{k-1}}$ } .

In my symbols, let order of α be n so that $\alpha^n = 1$ and n is smallest. So I have this list of exponents, and for sure each one can be written as some α^m where m is from 0 to 1-1, and I think this m is the "residue". So basically

"residue module n of exponent" = Rem(exponent/n).

For example, if $\alpha^{15} = 1$, then $\alpha^{16} = \alpha^1$ and 1 is the residue of 16.

Here is another possible meaning of "residue" :

residue modulo f(x) of x^4 = Rem(x^4 / f(x))

This is not really the same usage exactly, but I get the point. In the second usage, residue is just the usual remainder.

OK, I give up on the method they outline involving all this residue stuff. I don't think it contains anything new even if I could decode the language. I am more interested in the table. Here is part of it

```
DEGREE    2        1  7H

DEGREE    3        1  13F

DEGREE    4        1  23F       3  37D       5  07

DEGREE    5        1  45E       3  75G       5  67H

DEGREE    6        1  103F      3  1278      5  147H      7  111A      9  015
     11   155E    21  007

DEGREE    7        1  211E      3  217E      5  235E      7  367H      9  277E
     11   325G    13  203F     19  313H     21  345G
```

The number in front of each octal deal is the power of $(x-\alpha^i)$ in the first factor of the min poly. This then lets you use the general rule to wrote out the factored form I think using the usual exponent sequence.

I can compare this to my own stuff. When I list off all min polys for GF(2^3) I get

GF(2^3)

$$\begin{aligned} p_1(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^4) &&= x^3+x+1 \quad = 1011 = 13_8 \\ p_3(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^5) &&= x^3+x^2+1 \end{aligned} \tag{6.20}$$

So this is his table item 13F. He earlier says

```
A, B, C, D    Not primitive
E, F, G, H    Primitive
```

Idea: If a polynomial has degree < m, I know it can still be a min poly. I think he only puts the above letters on min polys that have the full degree m.

so yes, this is primitive. Next,

GF(2^4)

$$\begin{aligned} p_1(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) &&= x^4+x+1 \quad = 10011 = 23_8 \\ p_7(x) &= (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11}) &&= x^4+x^3+1 \quad = \text{partner of above} \\ m_3(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) &&= x^4+x^3+x^2+x+1 \quad = 11111 = 37_8 \\ m_5(x) &= (x-\alpha^5)(x-\alpha^{10}) &&= x^2+x+1 \quad = 111 = 7_8 \end{aligned} \tag{6.21}$$

For some reason he puts no label on this 07 one, why is that? It is not of degree 4, that is true. I would say it was "not primitive" since not even the right degree, but I guess that is obvious. See idea above.

So I understand his table. Now let's ponder GF(2^6) which is one I did not do and has $2^6-1 = 63$ which factors and is therefore interesting. He has

```
DEGREE     6         1   103F       3   1278       5   147H       7   111A       9   015
      11    155E     21   007
```

For example

103 = 001000011 = 1+x+x^6

I think for the first time here, I am doing Maple code to compute the period of some h(x).

I run this into my little Maple searcher for the period and find

```
h := 1 + x + x^6;
```

$$h := 1 + x + x^6$$

```
for n in divisors(p^m-1) do
  print(n, Rem(x^n-1,h,x) mod 2):
od;
```

$$63, 0$$
$$1, x + 1$$
$$3, x^3 + 1$$
$$7, x^2 + x + 1$$
$$9, x^4 + x^3 + 1$$
$$21, x^5 + x^4 + x^3 + x$$

Thus the period is 63 since this is the smallest one that works, and that is the case for any primitive one, His next one is 1278 which doesn't even make sense, it might be 127B. Let's skip that one.

Next is

111A = non prim =001001001 = 1+ x^3 +x^6

```
h := 1 + x^3 + x^6;
```

$$h := 1 + x^3 + x^6$$

```
for n in divisors(p^m-1) do
  print(n, Rem(x^n-1,h,x) mod 2):
od;
```

$$1, x + 1$$
$$3, x^3 + 1$$
$$7, x^4 + x + 1$$
$$9, 0$$
$$21, x^3 + 1$$
$$63, 0$$

So this one has period = 9. Next

$015 = 001101 = 1 + x^2 + x^3$

```
for n in divisors(p^m-1) do
  print(n, Rem(x^n-1,h,x) mod 2):
od;
```

$$1, x+1$$
$$3, x^2$$
$$7, 0$$
$$9, x^2+1$$
$$21, 0$$
$$63, 0$$

and this one then has period 7. Next,

$007 = 111 = 1 + x + x^2$

```
h := 1 + x + x^2;
```

$$h := 1 + x + x^2$$

```
for n in divisors(p^m-1) do
  print(n, Rem(x^n-1,h,x) mod 2):
od;
```

$$1, x+1$$
$$3, 0$$
$$7, x+1$$
$$9, 0$$
$$21, 0$$
$$63, 0$$

So this one has period 3. That is all the non prims. So here is a list

			α^k	
103	$1+x+x^6$	period = 63	α^1	order = 63
111	$1+ x^3 +x^6$	period = 9	α^7	order = 9
015	$1 + x^2 + x^3$	period = 7	α^9	order = 7
007	$1 + x + x^2$	period = 3	α^{21}	order = 3

So now I have a period column and I know the first element of the min poly. *The order column will be added next* and I will use

[order of β] = n/GCD(k,n) where $\beta = \alpha^k$ n = 63

So the idea that order = period persists through the case GF(2^6) !!!

So I am starting to think my little theorem might actually be true since lots of examples have order = period.

The case of GF(2^{12}) has as much RICHER variety of non-prim polys.

Maple problems

(1) How can I enter something like 321_8 and have it convert that to a decimal number 3*64+2*8+1 = 209.

- Here is one way:

```
c := convert([1,2,3],base,8,10);
```

$$c := [9, 0, 2]$$

.

where all ordering is backwards and I have to enter the number backwards.

- Here is another way

```
o := [3,2,1];
```

$$o := [3, 2, 1]$$

```
o[1];
```

$$3$$

```
L := nops(o);
```

$$L := 3$$

```
d := sum( o[i]*8^(L-i), i=1..L);
```

$$d := 209$$

At least this way I can enter the octal digits in a natural order.

I have now **written a Maple program** where you enter the WP octal thing and it computes the order and the period, and they ALWAYS come out the same, I tried some m = 12 cases. Maybe this is always true for p = 2.

So I guess I better find a proof! I am on my own here, have no idea how I would look this up somewhere. I think maybe I have it.

HERE IS MY PROOF!!

Done need this part

Aside: Here is another way to show cannot have N > n. Suppose that were the case. Then we have

$\alpha^{N} = \alpha^{n}\ \alpha^{N-n}$

$1 = 1\ \alpha^{N-n}$

$\alpha^{N-n} = 1$

But since N is the order of α, there cannot be some smaller integer N-n such that $\alpha^{N-n} = 1$. So we can rule out the case N > n.

So here is the Fact and Proof:

Fact: If h(x) is any minimum polynomial of GF(q) of degree k, then the *order* of any member of the conjugate set of h(x) equals the *period* of h(x).

Proof: First of all, we know from (5.35) that all members of such a conjugate set have the same order, which we shall call N. Recall that the order of some α in GF(q) is the smallest integer N for which $\alpha^{N} = 1$. The period, on the other hand, is the smallest integer n such that h(x) divides evenly into $(x^{n}-1)$, so $(x^{n}-1)/h(x)$ = some polynomial g(x) with no remainder.

The k elements a_i of the conjugate set of h(x) comprise all the roots of h(x), so $h(a_i) = 0$ for any conjugate set element. Since these are *all* the roots of h(x), if one finds that h(β) = 0, then β must be one of the conjugate set elements. We know that h({x}) = 0 because we know {h(x)} = 0 since there is no remainder when h(x) is divided by h(x) in the representation $GF(p^{m}) = R/h(x)$. Since h({x}) = 0, we conclude that {x} must be one of those a_i conjugate set elements. Therefore, the order of {x} is N. We now denote this particular a_i root by the name α.

Now consider these steps:

$g(x)h(x) = (x^{n}-1)$ // period n is the smallest integer that makes this possible

$g(\{x\})\ h(\{x\}) = (\{x\}^{n}-1)$ // apply {...} to both sides and use the rules of (3.14)

$g(\alpha)h(\alpha) = (\alpha^{n}-1)$ // {x} has name α

$0 = (\alpha^{n}-1)$ // since h({x}) = h(α) = 0

$\alpha^{n} = 1$.

Thus, we see that n is a *candidate value* for N, the order of {x} = α and all other conjugate set elements. Since we are finding here that $\alpha^n = 1$ for period n, we certainly know that the order $N \leq n$ since N is supposed to be the smallest possible integer for which $\alpha^N = 1$. Thus we have ruled out N > n.

We shall now also rule out N < n and conclude therefore that N = n.

Suppose N = order of α = {x} and n = period of h(x) with N < n. Since the order is less than the period, we must get a non-zero remainder r(x) when (x^N-1) is divided by h(x),

$(x^N-1)/h(x) = q(x) + r(x)/h(x)$ or $(x^N-1) = q(x)h(x) + r(x)$ where $r(x) \neq 0$.

This says that $(\{x\}^N-1) = r(\{x\})$ or $(\alpha^N - 1) = r(\alpha)$ where α = {x}. But since N is the order of α, we know that $\alpha^N = 1$ so we then find that r(α) = 0, but $r(x) \neq 0$, and the degree of r(x) is < k.

We assumed that h(x) was the minimum polynomial for α. Thus, h(x) has this form:

$h(x) = (x-\alpha)(x- a_1)(x-a_2).....(x-a_{k-1})$ h(x) in R, all a_i in GF(q), deg h(x) = k

Since r(α) = 0, it has this form:

$r(x) = (x-\alpha)\ (x-b_1)(x-b_2).....$ r(x) in R, b_j = unknown but in GF(q), deg r(x) < k

Both h(x) and r(x) have the form for a minimum polynomial of α, but since r(x) has the lower degree, it must be the true minimum polynomial of α which then has degree < k. But this contradicts our original assumption that h(x) is the minimum polynomial of α and has degree k. Therefore we cannot have N < n.

The conclusion is that n = N so the period n of a minimum polynomial is the same as the order N of any of the elements of the conjugate set of that minimum polynomial.

Comment: If irreducible h(x) in R degree k < m is *not* a minimum polynomial of GF(q) (white region of Fig 5.5) , then it cannot be written in the usual factored form shown above, and therefore it cannot divide into $x^n - 1$ for any n, even for n = q-1. Such a polynomial therefore has no period whatsoever. Of course it also has no conjugate set, so we cannot talk about the order of conjugate set elements. The point is just that if h(x) is not a minimum polynomial, this Fact makes no sense at all.

Here are some notes *before* the above was found and I am flailing away with various "plans".

Again: could it be that n > N ? In this case

$\alpha^n = \alpha^N\ \alpha^{n-N}$

$1 = 1\ \alpha^{n-N}$

$\alpha^{n-N} = 1$

I am now stuck at 5:45 PM June 29, 2013. I don't see how to rule out this possibility, but I just know that it is not possible because I looked at lots of min poly cases. I am missing some ingredient!

Plan A. Assume that N > n. For example, suppose $p^m-1 = 63$ and we have {1,3,7,9,21,63} as candidates, and suppose order N = 3 and period n = 9. Then it must be that we get a non-zero remainder here:

$(x^3-1)/h(x) = q(x) + r(x)/h(x)$ or $(x^3-1) = q(x)h(x) + r(x)$ where $r(x) \neq 0$.

This says that $(\{x\}^3-1) = r(\{x\})$ or $(\alpha^3 - 1) = r(\alpha)$ where $\alpha = \{x\}$. But since order N = 3, we know that $\alpha^3 = 1$ so we then get that $r(\alpha) = 0$, but $r(x) \neq 0$.

Injected comment later: If $r(\alpha) = 0$ and $r(x) \neq 0$, then r(x) is a candidate for being a min poly of α. Clearly r(x) is of degree < k . But h(x) is supposed to be a min poly for α and has degree k. This is a contradiction, we cannot have such an $r(x) \neq 0$ when we put the order N = 3 into our equation.

Then the form of r(x) must be

$r(x) = (x-\alpha)\,(x-A)(x-B)...$ total degree < 3

Then since α is also a root of h(x) we get

$(x^3-1) = q(x)\,(x-\alpha)\,(x-A')(x-B')..\, +\, (x-\alpha)\,(x-A)(x-B)...$

$= (x-\alpha)\,[\;\; q(x)\,(x-A')(x-B')..\, +\;\; (x-A)(x-B)...\;\;]$

This says that α is also a root of $(x^3- 1)$ so $\alpha^3 = 1$, but we already know that.

Plan B. It must be something about h(x) that I am ignoring. Recall the general form for the exponents of the elements of conjugate set is this

exponents = $\{ s, sp, sp^2, sp^3, ... sp^{k-1} \}$. $= \{ \beta^s, \beta^{sp}, \beta^{sp^2}, \beta^{sp^3}, ... \beta^{sp^{k-1}} \}$.

I know that *every one* of these elements on the right has order N = 3 in my example

$h(x) = (x - \beta^s)(x - \beta^{sp})(x - \beta^{sp^2})....(x- \beta^{sp^{k-1}})$ degree k

where β here is a primitive element! One of these things is $\{x\} = \alpha$. Suppose all these conj elements have order N. Then I should be able to show that this is a no-remainder division

$(x^N-1)/\ \{(x - \beta^s)(x - \beta^{sp})(x - \beta^{sp^2})....(x- \beta^{sp^{k-1}})\} = g(x)$

which says

$(x^N-1) = g(x)(x - \beta^s)(x - \beta^{sp})(x - \beta^{sp^2})....(x- \beta^{sp^{k-1}})$

I want to show the above is true if I know that every conj element has order N. For example, $\beta^{Nsp^2} = 1$. Dead in the water!

Plan C. Maybe browse through GA looking at the various "proof methods" used. Maybe I will find some method I have forgotten about.

• I have not used the fact that $p\alpha = 0$ for any α in GF(q).

• [order of β^{sp^i}] = n/GCD(k,n) where $\beta^{sp^i} = \alpha^k$ and n = order of α. What should I take α to be? Suppose I select $\alpha = \beta$ which is a primitive element. Then I have

[order of β^{sp^i}] = n/GCD(k,n) where $\beta^{sp^i} = \beta^k$ and n = (order of β) = q-1

This seems to say that

[order of β^{sp^i}] = (q-1)/GCD(sp^i,q-1)

Now back up. Suppose n is the period and N is the order, then we have

$(x^n-1) = g(x)(x - \beta^s)(x - \beta^{sp})(x - \beta^{sp^2})....(x- \beta^{sp^{k-1}})$

N = (q-1)/GCD(sp^i,q-1) // this is the same for i = 0,1,2,,,k-1 !

I cannot relate this formula to the information of the previous line. But if the same for all those i values, let's consider i = 0 so then

N = (q-1)/GCD(s,q-1)

so I have now related order N to the s thing in those exponents of h(x). Still dead in the water.

• An idea from (4.25). The a_i here form a cyclic subgroup of GF(q).

$$x^n - 1 = (x - a_1)\bullet (x - a_2)\bullet (x - a_3)\bullet \ldots (x - a_n) . \qquad (4.25)$$

If I factor g(x) I would get

$$(x^n-1) = (x-g_1)(x-g_2) \ldots\ldots (x - \beta^s)(x - \beta^{sp})(x - \beta^{sp^2})....(x- \beta^{sp^{k-1}})$$
$$\qquad\qquad n-k \qquad\qquad\qquad\qquad k$$

and maybe all these factors form a cyclic subgroup of order n! A new idea at least. I don't know if this thing works in this direction, however. Next to the above one can always write

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

The previous line contains some subset of these factors.

- (5.4) seems interesting :

Fact 1: If p(x) lies in R and p(α) = 0, then p(x) = q(x)h(x) of α . In other words, p(x) having a root α must be a multiple of any minimum polynomial h(x) of α. (5.4)

The proof of this Fact suggests a new path

Plan A Revisited. Assume that N > n. For example, suppose p^m-1 = 63 and we have (1,3,7,9,21,63} as candidates, and suppose order N = 3 and period n = 9. Then it must be that we get a non-zero remainder here:

$(x^3-1)/h(x) = q(x) + r(x)/h(x)$ or $(x^3-1) = q(x)h(x) + r(x)$ where $r(x) \neq 0$.

This says that $(\{x\}^3-1) = r(\{x\})$ or $(\alpha^3 - 1) = r(\alpha)$ where $\alpha = \{x\}$. But since order N = 3, we know that $\alpha^3 = 1$ so we then get that $r(\alpha) = 0$, but $r(x) \neq 0$.

If $r(\alpha) = 0$ and $r(x) \neq 0$, then r(x) is a candidate for being a min poly of α. Clearly r(x) is of degree < k. But h(x) is supposed to be a min poly for α and has degree k. This is a contradiction, we cannot have such an $r(x) \neq 0$ when we put the order N = 3 into our equation.

Can I make this fly. Suppose N = order of $\alpha = \{x\}$ and n = period of h(x) with N < n (3 < 9 above). *Since the order is less than the period*, we get a non-zero r(x) here:

$(x^N-1)/h(x) = q(x) + r(x)/h(x)$ or $(x^N-1) = q(x)h(x) + r(x)$ where $r(x) \neq 0$.

This says that $(\{x\}^N-1) = r(\{x\})$ or $(\alpha^N - 1) = r(\alpha)$ where $\alpha = \{x\}$. But since N is the order of α, we know that $\alpha^N = 1$ so we then get that $r(\alpha) = 0$, but $r(x) \neq 0$.

If $r(\alpha) = 0$ and $r(x) \neq 0$, then r(x) is a candidate for being a min poly of α. Clearly r(x) is of degree < k. But h(x) is supposed to be a min poly for α and has degree k. This is a contradiction, so we cannot have the situation N < n.

It remains then to rule out the situation N > n.

Therefore, $(x^N-1)/h(x)$ must divide evenly where N is the order. It is possible that this might be true for some n < N as well.

If I can rule out the n < N case (period < order), we have it!!!