This is the Title PhL 3.26.05

First proofing:

Chapter 1

(a) done, and seems pretty clean.

(b) 1. OK
2. OK
3. OK, this was a harder, facts about cyclic subgroups of cyclic groups
4. additive cyclic groups
5 Example of the modulo group

(c) 1. OK. I am trying some humor to cut the boredom here.
2. OK
3. OK
4. OK, but things are getting denser now. Maybe we need some pix!
5. OK, I at least am giving simple examples of this abstruse stuff.
6. OK
7. OK

Something graphic is needed here, or some summary , or analogy

group G with operation * which could be *either* • or +
subgroup H of G
normal subgroup H
chart with rows as cosets, 1 column as coset leaders
rows {..} (cosets) are elements of the factor group G/H

ring R with both operations + and •
ideal I (subgroup of R for +; subring of R for • but also rI = Ir = I)
chart with rows as residue classes), 1 column as residue class leaders
rows {..} (residue classes) are elements of the residue class ring R/I

Question:

" If g is in an element of group G, then so is g*g = g^2, and (g*g)*g = g^3 , and so on. If the group has a finite number N of elements, you must, as you keep increasing this power, come to a point where g^n = 1. "

Why is that true?

OK, I have added new stuff to the opening section of Chapter 1 to make things clearer. They were just NOT clear at all I am afraid.

Fri Jan 11, 2013. OK, I have been through Chapter 1 a few times now, editing each time. I have verified every single item and I think I "grok" the whole thing pretty much. Let's now move on.

Chapter 2

(a) OK finally at 2 PM.

(b) OK at 2:35 PM, so chapter 2 went pretty fast.

Chapter 3

(a) OK

(b) OK

(c) OK, it is getting a bit mind bending now.

(d) OK and pretty good in terms of pace and climactic content with rim shots.

(e) OK

Status: as of 4 PM 1.11.13 I have blasted through the first three chapters of galois doc. The first chapter was the hardest I think.

Chapter 4

(a) OK

(b) OK

(c) OK

(d) continue here on Sat Jan 12. This is a brutal long section with a million details!

(e) an example, just in time, OK

(f) labeling using powers of α versus m-tyuples, OK

(g) selected facts

That was a heavy duty chapter!! But we are only 40% through the document!

Chapter 5

(a) OK

(b) OK, but I am glazing over, there is too much stuff coming at me.

(c) first cut

(d) first cut

(e) first cut

Sun Jan 13. I am torn about how to number things in this doc. Here is the current status

Chapter 1:	maybe 6 Facts's, not numbered.
Chapter 2:	some Facts are called Claims, maybe 8 Facts total, not numbered
Chapter 3:	some Facts are called Theorems, maybe 3 total, not numbered
Chapter 4:	2 Facts, then Facts 1 through 16 plus some Theorems, then four final Facts
Chapter 5:	Facts numbered through 15, then some Theorems.
Chapter 6:	3 Facts no numbers
Chapter 7:	very confused, each subsection has its own numbered facts/

OK, I started all over again with my editing proofing pass. This time I have more "equation" numbers than ever, Proof is just underlined, the word Definition is removed, defined items are in bold the first time they appear, and even these definitions tend to get equation numbers. So things are more "uniform" in

terms of style and notation. But as of 3 PM, I have only been able to do Chapter 1! It now has 45 equations. I repaired many logic flaws and some mistakes. This Chapter runs from p 2 to p 20 and so accounts for 19/113 = 17% of the document. The subject of Modern Algebra is very difficult for me and very foreign.

I have reached the end of Chapter 2 with all the new formatting and numbering. It is once again "OK".

I have reached the end of Chapter 3 with all the new formatting and numbering. All OK.

1. Modern Algebra	pp 3-20	18p
2. Galois fields GF(p)	pp 21-25	5 p
3. Polynomials	pp 26-31	6 p
4. Galois Fields GF(p^m)	pp 32-46	15 p

a,b,c,,d all OK continue here tomorrow.

Mon Jan 14.

4. Galois Fields GF(p^m)	pp 32-46	15 p

e, added a long but good comment about the two meanings of "x"

f,g finally all OK

5. The Minimum Polynomial

(a) OK, it is defined and seems clear.

(b) OK, equations numbered.

In the middle of (c), I went off and processed **Appendix B** which took a very long time!! 4PM.

(c) OK

(d) OK, but a shabby conclusion with a bunch of probably dead references.

(e) maybe delete this, for now let's continue on.

At this point I did several things

- first cut reading of all of Chapter 6
- section reformatting of Chapter 7 and 8

Tues Jan 15.

A review of some facts:

1. In the R/I business, the f(x) polynomial is taken monic and of degree m with coefficients in GF(p). There are m coefficients possible for the other terms (**first term is x^m**) so there are p^m possible polynomials of this class f(x). Each one can be used in the R/I sense to produce a ring. When *any* polynomial is *divided* by f(x), the remainders are polys of degree m-1 which have m coefficients each of which can take the p values of GF(p), so there are **p^m possible remainders**.

2. This f(x) is **irreducible** if it cannot be factored into a product of polynomials each of which has coefficients only in GF(p). If an irreducible f(x) is used in the R/I thing, the resulting object (rows of chart) form a field which is a representation of GF(p^m). Leading term is x^m. In this case, each row of the

chart is represented by some remainder polynomial and written $\{r_i\}$ and these rows are then thought of as elements of GF(p^m).

3. A **minimum polynomial** m(x) for α in GF(q) is the smallest set of factors $(x-a_i)$ which includes (x-α) as one of the factors (and where all the a_i are in GF(q)) and which, when multiplied out, has all coefficients in GF(p). Clearly m(α) = 0. The minimum polynomial for α is unique (5.5). Since a minimum polynomial cannot be "factored in GF(p)", any minimum polynomial is also an irreducible polynomial.

This m(x) could have degree as low as 1 if (x-α) were the only factor, in which case α would have to be in GF(p). In theory, one might have a factor for every element of GF(q), so then m(x) would have degree q. We know from Big Theorem 2 that this polynomial is $x^q - x = (x^{q-1}-1)*(x-0)$. If α = 0, then we have to keep the (x-0) factor in m(x) and it would indeed have degree q. For any α ≠ 0 in GF(q), the largest possible minimum polynomial would be $x^{q-1}-1$ which has degree q-1. In principle a minimum polynomial for α ≠ 0 could in theory have degree anywhere from 1 to q-1.

It turns out that in fact the degree of a minimum polynomial for α ≠ 0 in GF(p^m) cannot run the full range 1 to q-1. The degree (call it k) must lie in the range 1 to m. Big Theorem 3 (5.17) gives an explicit formula for the k factors of a minimum polynomial, though k must be determined by "experiment".

If the degree of a minimum polynomial is less than m, it obviously cannot serve as the f(x) which is used to make the polynomial representation of GF(p^m), since f(x) to do that must be of degree m.

Since $x^{q-1}-1$ is the product of factors $(x-a_i)$ where a_i are all non-zero elements of GF(q), we know that whatever the minimum polynomial of α is, it must divide evenly into $x^{q-1}-1$. However, the minimum polynomial *might* also divided into x^n-1 for some n less than q-1. The smallest n is called the **period** of α.

4. It turns out that GF(q) - 0 is a cyclic group under • and therefore this group must have at least one generator α which can enumerate all the non-zero elements of GF(q) as powers of α. Such an element α of GF(q) is called a **primitive element**. Obviously a primitive element α cannot be the 0 element.

5. If α is a primitive element of GF(q), then the minimum polynomial for α is called a **primitive polynomial**. Since α ≠ 0, in theory a primitive polynomial could have degree from 1 to m, since it is a minimum polynomial of α. Any primitive polynomial is a minimum polynomial as well as an irreducible polynomial.

It turns out that a primitive polynomial always has degree m and the full period n = q-1. Thus, any primitive polynomial is suitable as f(x) in the R/I representation of GF(p^m). For some GF(q), there might be several primitive polynomials for several different α's.

Repair: the highest power in a polynomial is its degree, not its order. Added note on this and fixed a few located wrong uses of the word order.

Maybe make a definition index??

Chapter 6.

(a) added some meta comments, this review now makes complete sense to me, so I can proceed.

Improved proof for (5.5) (a).

Had an Alta crash at this point and had to do recovery work, see notes, think we are back. I was not frequently saving and had to pay for that mistake!

Chapter 5

(e) I have finally finished this section. I had to learn a little in Chapter 6 to verify this stuff. All OK.

Chapter 6

(a) OK

(b) OK

Chapter 7

(a) well, I got started into this new chapter, first cut reading, totally different topic. Time needed!

Weds Jan 16.

Chapter 7

(a) it took me ALL DAY to get through this subsection. I had to rewrite a lot of things, and I had to remove all the clumsy • matrix symbols. Many proofs were illogical. Oy, a long haul this is.

(b) just read some of this section to but the ice a little. It is all very good stuff IIDSSM.

Thurs Jan 17.

This entire day went to figuring out what I meant by saying that the GF(1) elements are vectors in some vector space. I had this wrong. I have now rewritten section 1 (b) 4 and there are a few more things I have to add in later sections. Then I can get back to the code stuff an its vector spaces!

Fri Jan 18.

Reviewed Section 1 (b) 3 on cyclic groups and fixed more errors.
Reviewed Section 1 (b) 4 on additive and additive cyclic groups and vector spaces.

Added planned info on GF(p) and GF(q) for both vector space and additive cyclic concepts.

Chapter 7:

(a) in progress at lunch break

Sat Jan 19.

Second power crash required CMOS and fan replacement, and may still not be fixed. It stopped progress yesterday, hope to be able to move forward a bit today.

Chapter 7
Section a

(a) 1 is OK

(a) 2 is OK

(a) 3 is OK

(a) 4 is OK

Section b
(b) 1 is OK.
(b) 2 is OK
(b) 3 is OK
(b) 4 is OK on CRC
Section c is OK.
Section d is OK. Breaking new ground now.
Section e first cut
Section f first cut, I have had enough for today.

Sun Jan 20.

I decided to break the 34 page long Chapter 7 into Chapters 7,8,9. The equation number count was getting just too high, raising the cost of readjusting the numbers. The new Chap 7 on Block Code just by itself has 37 equation numbers! I think this improves the overall structure of the document. I did not know how MUCH stuff was jammed into this last Chapter 7 before splitting.

I added two notational remarks, one on the first-index convention, and a second on which symbol comes first. I don't feel the need to completely review the *new* Chapter 7 because I have done that several times. I will start today's review with the new Chapter 8.

Chapter 8
(a) OK
(b) OK
(c) OK
(d) OK
(e) OK
(f) OK
(g) OK
(h) OK, a big payoff on error correction, added to section title feeding time
(i) OK and that is the end of a good Chapter 8 IIDSSM

Chapter 9
(a) OK, it is simple and clear despite the strange theorem.
(b) well, I got down to a certain point today after much pain. Am out of steam at 8 PM.

Mon Jan 21.

Reviewing once again Chapter 8. On each pass improvements are made.

Chapter 8
(a) OK
(b) OK
(c) OK
(d) OK on CRC
(e) OK on the one to one, just scanned this,
(f) OK on why cyclic code is cyclic, scan only, seems good

(g) OK, but harder since ideal and ring. Seems that some proofs are missing somewhere.
(h) OK on std array and our first real EC method
(i) OK on the connection

This really is an excellent chapter, I am very happy with it.

Chapter 9
(a) STOP

When I got up to the LCM thing for BCH, I was forced to add a bunch of useful Facts to the end of Chapter 5 on min polys. Since this was at the end of Ch 5, no equation numbers in Ch 5 got changed.

Tues Jan 22.

Added Section 8 (j) on motivation for g(x) coefficients in GF(p). Linked to it from the min poly chapter. Time to move on.

Chapter 9
(a) interruption

I worked on the GF(q) table stuff and added some tables from the web for $2^{3,4,5}$ which will probably be useful to someone, and which at least makes a connection to the outside world. I now would like to find a source of min poly's other than just Rhee p 171 for my one case, and this will take some effort. Thus, I am on hold at a certain point in 9 (e), more research needed here.

I have ended up doing it myself, and this is adding more to the document. I showed for GF(2^5) how you can find all the minimum polynomials, I think ! It was very enlightening, but I am confused a bit at 9:15 PM so time to shut down for the day.

http://www.commsys.isy.liu.se/en/staff/mikael/polynomials/primpoly

The above is an important link to primitive poly lists!

Weds Jan 23.

Cleaned up the three examples of Ch 5, they are much better now.

Question: Is it possible to have a monic polynomial over GF(2) which cannot be factored over GF(2^m) ?

I have never addressed this question anywhere. As an example, for GF(2^4) we have these polys

$x^4 + x^3 + x^2 + x + 1$ divides into $x^5 - 1$ so flunks period test
$x^4 + x^3 + x^2 + 1$
$x^4 + x^3 + x + 1$ $= (x^3+1)(x+1)$ = reducible
$x^4 + x^2 + x + 1$

$x^4 + x^3 + 1$	°	10011	
$x^4 + x + 1$	•	11001	
$x^4 + x^2 + 1$			
$x^4 + 1$		$= x^4 - 1 = (x-1)(x^3+x^2+x+1)$ = reducible	(5.31)

I know for complex numbers they could all be factored.

Consider $x^4 + x^2 + 1$. If it could be factored, then it would be a minimum polynomial for some α -- any of the α's that were in the linear factors. It is irreducible in GF(2) which it appears to be, then it must be the min poly for some α. Example GF(2^4) shows there are 3 min polys of degree 4, two of which are primitive. This poly then *could* be that third min poly, so it might be factorable.

Question: How can I do GF(2) division in Maple?

Answer: I learned how from here http://www.math.nmsu.edu/~pmorandi/math431s02/Polynomials.html

It is in fact quite easy, Maple knows about this subject.

At 5:45 I am sitting above equation (6.7) and I am not really happy with my vague "coordinate system" comments in those two paragraphs.

I am going to get rid of this entire comment, I cannot support it. Changing f changes the ideal, and I don't thing the coordinate system analogy really works.

****

Comment about f(x) and the m-tuple representation of GF(q) field elements.

One can think of a polynomial $f(x) = \Sigma_{i=0}^{m-1} f_i x^i$ as being a vector in a function vector space whose axes are powers of x. That is, 1, x, x^2, x^3.. x^{m-1} are the basis vectors (axes) of this vector space. One can then think of the coefficients f_i as forming a vector **f** in the space $[GF(p)]^m$.

The coefficients of a polynomial f(x) which form our m-tuple representation are the components of the vector f(x) along these axes, so one can think of the m-tuple of coefficients as being this vector f.

One can think of an m-tuple as a vector in a vector space over the base field GF(p), where the "digits" of the m-tuple are the components of the vector. The values of the vector components depend on the selection of "axes" in the vector space, and those axes are dependent on the choice of the f(x) used in the R/I residue class representation of GF(q). Changing from one defining f(x) to some other f(x) is like changing or rotating the coordinate system to some other set of axes. It is well known that problems are easier to handle in some coordinate systems than in others. For example, a problem with cylindrical geometry is often very difficult to solve in spherical coordinates.

****

I am running low on time now at 6:30 pre pub. I want to automate these tasks

(1) how to build "the table" of Chapter 6 **DONE**

(2) how to build the conjugate lists and then get all min polys in factored form (Ch 5 task) **Added comment that this would not be hard.**

(3) how to convert these to simple x^2+x+1 type form. **DONE**

Then I want to verify this with the web somewhere. Also

(4) how to you get a prim poly so you can get the ball rolling? **OK**

(5) when you get your list of min polys as in (2), how do you know which ones are prim polys? **My three Ch 5 examples show how you do this.**

Lots of loose ends floating around here.

Fri Jan 25.

No entry from yesterday. I have been adding Maple stuff to Ch 6 and making connections between Ch 5 and Ch6. Things are so shuffled now, I am going to reread Ch 5 and Ch 6

Chapter 5 a,b,c,d,e,f DONE. I did not read any proofs, just the logic flow. Equation and Fig numbers all fully checked. But not all references to other equations checked.

Chapter 6 a,b,c,d 1,2,3,4,5 DONE.

Equation number check for Ch 6: repaired and done.

Question: why was it necessary to talk about the object {x} ? I do this, but could I have skipped it?

I start this subject at (6.1) in order to make a connection between GF(q) and Polys[x,GF(p)] / (f(x)). Did I develop this topic anywhere earlier?

R/I mentioned in (5.29) with a sort of verbal review of how you might pick some f(x) and construct + and • tables as in (4.14). I imply that we must really now how to create those + and • tables in the general case. (4.14) was in the m-tuplet basis. It is true that around (4.15) I play a bit with 'x'. For GF(4) I easily find the prim poly in (4.13). I imply all the R/I stuff but never say it for some reason. So m-tuple really is the same as poly!

Does Section 4 (b) even know about R/I? I do mention it above (4.6). So I really am writing in this context. I then show details of $r_a(x)$ $r_b(x)$ remaindering.

OK, what I did in Ch 4 (b) is precisely the R/I stuff I do in 6 (b), so I have added a comment that we are now doing it for real.

OK, I guess I am happy with Ch 5 and Ch 6. I have certainly done a lot of fiddling there!

Next: I want to make sure my narrow-sense BCH back-references are good. I will start now here:

Chapter 9
(a)

Question: Why do people ignore the (31,1) code? Rhee's comment page p 172 says the code is "undefined" because it only has 32 field elements. So what? P&W do not show these entries in their page 274 long list of BCH codes, but they make no comment. Here is a guy who includes k = 1

1. To determine the dimension and generator polynomial of all narrow sense binary BCH codes of length $n = 31$, we have to do coset decompostion of the set $\{0, 1, 2, ..., 30\}$ mod 31 under multiplication by 2. It can be verified there would be six cosets each with 5 elements and one coset $\{0\}$. In other words $x^{31} + 1$ can be factorised as follows:

$$x^{31} + 1 = (x + 1)M_{\alpha}(x)M_{\alpha^3}(x)M_{\alpha^5}(x)M_{\alpha^7}(x)M_{\alpha^{11}}(x)M_{\alpha^{15}}(x),$$

where α is a primitive element of $GF(32)$. The degree of each $M(x)$ is equal to 5. The possible degrees for the generator polynomial for narrow sense BCH code are as follows:

$$(n - k) = 5, 10, 15, 20, 25, 30.$$

Therefore, the possible dimensions for the code are as follows:

$$k = 26, 21, 16, 11, 6, 1.$$

For the k = 1 code, there are 32 distinct symbols, the code words are huge 31 symbol things, and we can correct up to a 15-symbol error. I don't see any reason to throw this code out. Maybe good for a very low data rate of super important information. Probably it does not rate high on performance compared to other codes.

OK, I have finally moved the "ok to here" point a little forward in the BCH code chapter. Hopefully I can move forward at some better rate now. I note that my matrix appendix is huge, and maybe it will get eliminated. But for now, let's finish the codes stuff! Signing off at 8:30 PM Friday.

Sat Jan 26.

Need to understand this Hamming code p>3 issue.

Confusion #1. Are the coefficients of polynomials like d(x), g(x), c(x) in GF(q) or in GF(p)?

(1) When I write GF(p^m) = Polys[x,GF(p)] / (f(x)), I am saying that the elements of GF(q) can be represented by remainder polynomials whose coefficients are in GF(p). If you consider the remainders which are just constants in GF(p), those remainders represent GF(p) which is a subfield of GF(q).

But these are not the polynomials d(x), g(x), c(x)!!! These polynomials are not the remainder polynomials with GF(p) coefficients which represent elements of GF(q). Drill that in please!

(2) In the block code section, the components of vectors c and d and matrix G are all in GF(q).

(3) In the cyclic code section, the coefficients of c(x) g(x) and d(x) all lie in GF(q). The code word polynomials c(x) are found to be an ideal within $A_n \equiv$ Polys[x, GF(q)] / (x^n - 1) , notice GF(q).

I have now started a separate doc to try and reconstruct what I had to say about Hamming codes. It has been very rocky, but I think I have at least begun as of lunch break noon.

Question: Consider GF(2^4). The elements may be regarded as nibbles. There are 16 nibbles in this field. One of those bytes is 1000 (put LS on left). We can enumerate the 15 non-zero elements of GF(2^4) by powers of some primitive element α. So we have α, α^2,α^3....α^{15} . The question is: how would we associate these powers with the bytes?

Possible Answer #1. This is what the Table tells us! Recall

$$i^\lambda = \alpha i^3 + \beta i^2 + \gamma i + \delta.$$

λ	α	β	γ	δ
1			1	0
2		1	0	0
3	1	0	0	0
4			1	1
5		1	1	0
6	1	1	0	0
7	1	0	1	1
8		1	0	1
9	1	0	1	0
10		1	1	1
11	1	1	1	0
12	1	1	1	1
13	1	1	0	1
14	1	0	0	1
15				1

In the convention of this table, we then have

α = {x} = 0010 // different from my convention, I maybe should change it!

α^6 = 1100

So this is the answer to the question!

Question: If you ignore multiples, how many m-tuples are there for GF(p^m) ?

Use m = 4 for the moment. Then we will have

$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}\begin{pmatrix}2\\0\\0\\0\end{pmatrix}.....\begin{pmatrix}p\text{-}1\\0\\0\\0\end{pmatrix}$ = p-1 m-tuples, of which p-2 are multiples of the first

Since there are 4 places for the 1, this accounts for 4*(p-1) m-tuples

$\begin{pmatrix}1\\1\\0\\0\end{pmatrix}\begin{pmatrix}2\\2\\0\\0\end{pmatrix}$ etc = p-1 m-tuples, of which p-2 are multiples of the first

Since there are (4,2) = 12 places for the 1's, this accounts for 12*(p-1) m-tuples

$\begin{pmatrix}1\\1\\1\\0\end{pmatrix}$ etc = p-1 m-tuples, of which p-2 are multiples of the first

Since there are 4 places to put the zero, this accounts for 4*(p-1) m-tuples .

$\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$ etc = p-1 m-tuples, of which p-2 are multiples of the first

This accounts for 1*(p-1) m-tuples.

$\begin{pmatrix}1\\2\\0\\0\end{pmatrix}\begin{pmatrix}2\\4\\0\\0\end{pmatrix}$ etc

I think this is not a simple question! Here is the rule for two m-tuples to be multiples

Fact: Consider two m-tuples $\begin{pmatrix}a\\b\\c\\d\end{pmatrix}$ and $\begin{pmatrix}a'\\b'\\c'\\d'\end{pmatrix}$. For these to be multiples, there must exist an integer s in the range s = 2,3...p-1 such that

a = sa'
b = sb'
c = sc'
d = sd'

Sun Jan 27.

I have now written and installed the modified Hamming section, so I am now up to RS codes in chapter 9. I think the mod Ham section is not bad. It ties closely to the regular Ham section.

(d) Reed Solomon -- went very fast, wow, I had forgotten this major stuff
(e) also fast!

The first element of a *CIRC* decoder is a relatively weak inner (*32*,*28*) *Reed-Solomon* code, shortened from a (255,251) code with 8-bit symbols. This code can **...**

> For error-correction the information is broken up into segments called *frames*, where each frame holds 24 data symbols. The code used for error-correction is a *Cross Interleaved Reed-Solomon code* (CIRC) obtained by a process called "cross-interleaving" of two shortened Reed-Solomon codes, as described below. The 24 symbols from $\mathbf{F}_{2^8}$ from six samples are used as information symbols in a (shortened) Reed-Solomon $[28, 24, 5]$ code C_1 over $\mathbf{F}_{2^8}$. Another shortened Reed-Solomon $[32, 28, 5]$ code C_2 also over $\mathbf{F}_{2^8}$ is then used in the interleaving process, which has four additional parity-check symbols. See [7, 16, 17] for a detailed description of this process.

Corollary: The relation between t and d is d = 2t+1 if d is odd, and d=2t+2 if d is even. (7.33)

$d \leq n-k+1$ best you do is d = (n-k)+1/

4 PM. I have finished off the RS section! I now want to reread my GF(p) motivator earlier, and then finally do the digital filter section.

6 PM. Confusion about the addition table.

(1) The coefficients of polys which represent GF(q) are in GF(p) [yes], forget about data coding polynomials. Thus, a "digit" in an m-tuple is a GF(p) element [yes]. Even if you are doing $q = 2^8$, a poly coefficient is just a bit. So digit = bit. Thus, the addition table [as in (4.8)] for GF(2^m) only does bitwise addition and could use an XOR gate independently for each bit or digit. [yes, if you used hardware to compute your addition table] A symbol in GF(2^8) might be 255 which in wires is 1111,1111. [yes] If I made a + table like (4.10) I claim XOR gates does it [yes]. But WHY is this so? Well, you are adding two polynomials like $f(x) = a + bx + cx^2$ and $f(x) = a' + b'x + c'x^2$ so a digit addition is b + b' which is a GF(2) thing, and GF(2) = Z_2. [yes]

The addition tables involve polynomials in R which has coefficients in Z_p, so all above is OK.

(2) What is the rule for adding two elements of G(2^4)? Each of the two elements is represented by a polynomial remainder $f(x) = a + bx + cx^2 + dx^3$... of degree 3 where a,b,c,d are just bits in GF(2). Thus, the addition rule really is just XOR gate addition, there is no carry. For example

$f_1 = 0001$
$f_2 = 0001$
sum = 0000.

This situation arises in my example (4.10) and this is also shown in p 27 Rhee with 0,1,2,3 labels.

This item is OK.

(3) Now consider $(c_1\ c_2\ c_3) = (d_1\ d_2)\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix}$ where the G elements are bits but the d_i and c_i are bytes. [OK] We have $d(x) = d_1 + d_2x$ for example where the coefficients d_i are bytes = symbols. [yes] Each byte could be represented by a poly of degree 7 over GF(2), that is true. We are adding elements of $GF(2^m)$ and I think here too bitwise addition it, just as I originally claimed, no carry.

If you add two elements of $GF(2^m)$ where each element is represented by a polynomial in R, then yes, you would have the XOR thing. We are still just computing addition tables for $GF(2^m)$ here.

Here is verification

2.1 Addition

Addition in the finite field of $GF[2^m]$ is relatively simple since there is neither carry nor borrow. This operation can be realised using bit-wise XOR, i.e. $C = A \oplus B$. However for simplicity the plus sign (+) instead of $\oplus$ is used throughout this paper. Shown in Figure 1, addition can be implemented using both bit-serial and bit-parallel methods. In a bit-serial technique, data are shifted in bit by bit serially in to an adder. Obviously, only a 2-input XOR gate is required. The operation is completed in m clock cycles. In a bit-parallel technique, m-bit data are parallelly fed into adders and the result is obtained simultaneously.

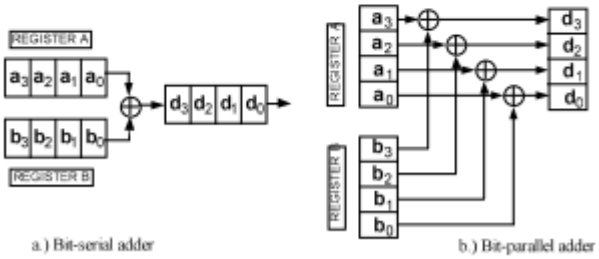


Figure 1 A bit-serial and a bit-parallel finite field adders

So I guess I will stick by my guns. I now think Chapter 8 (j) is right on the money. [wrong??]

Why wrong? In all of the above, we are talking about elements of GF(q) represented by polynomials in R which is the space of polys with coefficients in GF(p). But when we start talking block codes, we are talking polys with elements in GF(q), not GF(p) !! This is true for the regular block code discussion or the cyclic block code discussion. For example, in $(c_1\ c_2\ c_3)$ if $q = 2^8$ then each c_i is a code symbol and each c_i is a byte. In the cyclic world, c(x) has coefficients which are in $GF(2^8)$. This is R_q not the R used above and back in Chapter 3. In the code world, an m-tuple like (c_1, c_2, c_3) the thing c_2 is a byte. It is an

element of GF(256). If you add two m-tuples in this world, it is true that you add each symbol pair independently. But addition of each isolated symbol pair is done within GF(256) = GF(2^8). Note that GF(256) ≠ Z_{256} because this association is only valid if 256 were prime! See (2.5). Recall that GF(4) and Z_4 have different

So what does addition in GF(256) look like if you add two bytes? Each byte is a symbol, each byte can be represented by a poly in R with 8-tuple elements being bits. Two add two elements of GF(q), you can add these R polynomials, and YOU CAN DO XOR on the bits. So now I have flipped again on this subject ! It is addition in Z_{256} that requires the carry between bit lines, but we are not using this ring for our addition, we are using GF(256).

Now in light of that, go to the last digital filter section.

Chapter 10. This is my first time on this.

intro -- must be edited, but I am following things OK

(a) matrix review, all very clear and good, but format needs changing

(b) polynomials of a matrix -- all OK, formatting

(c) OK, I am fascinated, where is this heading!

(d) Example for skeptical. I want to see some A, and then get Maple to compute A^{511} !!

I did not have Maple when I wrote this thing perhaps.

I would really like to see a numerical set of matrices!!!

(e) wow.

OK, first cut is done. Now I have to ask: is this sitting out there on the web?

"galois field" "matrix representation" has 8270 hits, quite a few

"galois field" "matrix representation" cayley hamilton has 361 hits

There are papers in this search

"matrix representation of a finite field"

Well there is one paper by Wardlaw. It mentions the companion matrix with a reference.

I think he basically has it, so I guess I cannot claim much. But his paper is 1992, not all that old, and he is a Navy guy. He gives about 5 book references I don't have but maybe I should include.

The "companion matrix" is something in wiki even. It is the companion of a polynomial.

OK, I have read through this entire section, I will keep it in the doc for sure! I will not claim anything special for it. I don't have any obvious verification references. I think my effort is good and worth puttin out there.

Mon Jan 28. While working out Ch 10, I realize that certain Facts are missing from Chapter 3 about the notation {x} and so on. I will alter Ch 3 right now.

(a) I just did a full editing review of the matrix review section. I have decided not to number these things because I can refer to them as Fact 4 or whatever. There would be a very large number of equation numbers here. Many facts are irrelevant, but I will keep them anyway to make this a solid review for me or anyone else.

Then I cleaned up the opening text above (a).

Now working on (b). It is fine, and it now has equation numbers.

(c) This section is OK and numbered, but it is not clear what the point is. We conclude that a power of a matrix can be reduced to lower powers of degree < m. I guess C-H by itself does not say this. It lets you reduce A^m to lower powers.

(d) got it edited, took a long time, we are zeroing in!

OK, got to the end, but something is wrong with my equation for companion A, doing Maple, will fix manana. This is a good section.

Tues Jan 29.

OK, I got the Maple stuff into the end of Ch 10. I have a few extra tasks I would like to get in there

1. Fast way to search for primitive polynomials using the Rem function. I should do an example early on so reader knows it is always possible to find on. This would be a great addition to the paper I think.

Weds Jan 30.

Just reviewing now, wondering if what I did in Ch 10 is valid for p > 2. KJ at doctor.
intro-- will do later
(a) will do later
(b)

Question: Let d(x) be a prim poly for GF(p^m). Are the roots of d(x) all distinct? Well, the elements of the conjugate set are all distinct which is (5.15a)

Question: If p(α) = 0 where p(x) is primitive and α in GF(q), does that mean α is a primitive element? I think so, but where is my Fact stating this?

Question: Consider the GF enumerated as $\{0,1,\alpha,\alpha^2....\alpha^{q-1}\}$. Since this is a field, any of these field elements α_i must have an *additive* inverse which is an element of the list! How do you show this explicitly? What, for example, is the additive inverse of element α ?

http://www.dragonwins.com/domains/getteched/crypto/playing_with_gf%283%5E2%29.htm#The_elements_of_GF%2832%29_ tell us that

x^2+x+2 is a prim poly for $GF(3^2)$. So assume that $\alpha^2 + \alpha + 2 = 0$. We would use this to build up our little table

$\alpha^2 = -\alpha - 2 = 2\alpha + 1$ // from the primitive polynomial
$\alpha^3 = \alpha^2\alpha = (2\alpha + 1)\alpha = 2\alpha^2 + \alpha = 2(2\alpha+1)+\alpha = 4\alpha + 2 + \alpha = 2\alpha+2$
$\alpha^4 = \alpha^3\alpha = (2\alpha+2)\alpha = 2\alpha^2 + 2\alpha = 2(2\alpha + 1) + 2\alpha = 6\alpha + 2 = 2$
and so on.

So here are the results

α
$\alpha^2 = 2\alpha+1$
$\alpha^3 = 2\alpha+2$
$\alpha^4 = 2$
$\alpha^5 = 2\alpha$
$\alpha^6 = \alpha +2$
$\alpha^7 = \alpha + 1$
$\alpha^8 = 1$ (*)

Therefore here are all the inverses!

$-\alpha = 2\alpha = \alpha^5$
$-\alpha^2 = \alpha+2 = \alpha^6$
$-\alpha^3 = \alpha+1 = \alpha^7$
$-\alpha^4 = -2 = 1$
$-\alpha^5 = -2\alpha = \alpha$
$-\alpha^6 = -\alpha-2 = 2\alpha+1 = \alpha^2$
$-\alpha^7 = -\alpha-1 = 2\alpha+2 = \alpha^3$

This, to answer the question "what is the inverse of α^i", you first build the chart as in (*) above. Then you just look up each inverse!

This claim is made in the above web link

In GF(32), the number of primitive polynomials is exactly given by

$$N = \text{totient}(p^n-1)/n = 2$$

I have nothing like this in my doc.

Fri Feb 1. Did a little yesterday as well. I have now *greatly* simplified Chapter 10. Lots of confused roundabout information is replaced with a straightforward derivation of the matrix rep. Stopping at 3 PM since party action here tonight. It keeps getting better and cleaner, but I massive assembly of section rewrites lies ahead.

Sat Feb 2. Finally installed all the repaired chapters and we are back to a single galois doc again, but it needs massive proofing because many things have been shuffled. But I think all the material is in there now. I moved the matrix facts to Appendix C to make the reader of Chapter 10 suffer less.

I am going to work in the totient thing. From dragon

http://www.dragonwins.com/domains/getteched/crypto/playing_with_gf%283%5E2%29.htm#The_elements_of_GF%2832%29_

we saw this claim

$$N = \text{totient}(p^n-1)/n = 2$$

It is done! I even threw in a table. Decided to put this as a new little section.

Signing off at 9:30PM, did some reference work, could not find Chiffres (means statistics), but found a web link to first few pages.

Sunday Feb 3, 2013
Monday Feb 4, 2013

Reference for Modern Algebra? DONE.

Where to put QED and where not to? *********

Chapter 1 review:
equation numbers in order, there are 45 equations plus a,b,extras, all tabbed properly now.
no figures
pretext, OK added [1] B&M
(a) DONE, lots of small edits.
(b) 1, DONE
2, DONE, OK, removing you references in some places
3. DONE and OK
4. DONE and OK

5. DONE and OK
(c) 1, DONE and OK
2, DONE and OK
3. DONE and OK, pretty boring stuff.
4. DONE and OK, including the two little lemmas
5. DONE and OK
6. DONE and OK
7.DONE and OK

Chapter 2 review:
equation number sequence check OK
no figures
(a) DONE and OK
(b) DONE and OK. All equation numbers are being verified, very painful!

Chapter 3 review Polynomials
equation number sequence check OK
(a) DONE and OK
(b) DONE and OK
(c) DONE and OK

Question: back in Ch 3 (b): why is the ring R different from the ring $\mathcal{R}$?

$\mathcal{R}$ is the set of variables x. We could have $\mathcal{R}$ = GF(p) for example.

R is the set of polynomials in the variable x. Any polynomial f(x) in R lies in $\mathcal{R}$.
For example, f(x) = 2x + x^2 = (x + x) + x • x = y + z = w = element of $\mathcal{R}$.
Similarly any element of $\mathcal{R}$ forms a polynomial f(x) = x which lies in R.
So each set contains the other set!!! How can they be different? Snafu time!

AT 9 PM, I think my attempt to generalize things to some general $\mathcal{R}$ is falling apart. I invested this entire day (and several past days) trying to make it go, but it just complicates everything immensely. For example, you have to say that a minimal polynomial of α is one with (x-α) and which has coefficients in $\mathcal{R}$. That just means nothing at all when $\mathcal{R}$ is unspecified! Also I had to add my ugly "operational rule" just to make sense out of multiplying two polynomials.

If I back out now and get rid of $\mathcal{R}$, then I have to find some way to make Chapter 10 work! It is then no longer just a special case of all the earlier work!! So I guess I have to work now on Chapter 10 again and get it back spinning on its stick again! Too bad for me.

Tuesday Feb 5. Starting late at 10 AM after a sleepless night with constant heartbeat fear.

Will make a working copy of entire galois and fiddle in there today. I worked in "Trying again" all day, and I think things got better. I have developed some of the individual pieces, but I don't have the whole thing yet. Signing off at 7 PM due to bad sleep last night. Will try to read tonight, early in the sack.

Weds Feb 6 I continue in the Trying Again doc. I made a new Trying doc to put things in a better order. I now have these three new sections which will have to go somewhere:

(1) Specification of the ring R of polynomials with coefficients in Z_p
(2) The meaning of a polynomial in R being irreducible in R

In these sections, I no longer refer to a ring $\mathcal{R}$ which contains the variable x. I just say that x is inert, a carrier of coefficients, and x lies in some unspecified set. So this is a change.

(I also have a matrix section which I think will go into Ch 10, or will go nowhere.)

I have just read through **Chapter 4** on GF(q) in my working Feb 6 doc, and I did lots of edits. There is now no mention of $\mathcal{R}$, but there is also nothing which conflicts with the notion of x being an inert thing that is in some unspecified set! I avoid saying anything about x, and I certainly never say it is in Z_p nor to I say it is in GF(q) . Obviously if we have a root $x = a_i$ with a_i in GF(q), then that VALUE of x happens to lie in GF(q). I am scanning Galois doc now to make sure I am not getting into trouble by having x be this inert detached entity. Chapter 4 has passed this test, and now I will look at the critical Chapter 5. This will be important because this is where prim polys appear, and I need the prim poly concept in Chapter 10.

Reading through **Chapter 5**. Where I used to say f(x) is a polynomial over GF(p), I now say F(x) is in R. The first phrase implies maybe that x lies in GF(p) which I don't want to imply.

I stop now above Fact 7. Nothing I have seen so far is a problem.

I now need to **construct a new Chapter 3** that says the right things. I will do this in a separate doc called Chap 3 rewrite Feb 6. I have now done this. Polys[,,,,] is now replaced with R.

I will now install this new chapter 3 into the entire galois working Feb 6 and this will then become the actual main document!!

Chapter 3 is installed,
Lets go down Chap 4 again with quick cleanup.
Chapter 5 quick cleanup as well. Well, another battle, fixed the reciprocal, I think I have purged this thing of Polys(..) references.

I am now ready to attempt to climb Chapter 10. Single walk first.

Thurs Feb 7

I think the Ch 10 thread is now correct, but the logic flow needs improvement, things are not in the right order yet. // Did this, installed my new Ch 10. I now need to do some general file cleanup, things have piled up, then improve the maple part of Ch 10. Do a case with p > 2. I did it somewhere.

OK, I have finished the Maple work for matrix reps, but then I realized that my X_{p^m} ring might just be the set of possible remainders of matrix division and then I have said a lot of dumb stuff.

Question: is this set $\mathcal{X}_p^m$ the set of all possible remainder matrices when a matrix polynomial in R_p^m is divided by some d(x) of degree m?

Fri Feb 8.

Starting 3 PM after looking at the Beth PC. Will now read through Chapter 10.

Chapter 10

(a) did several passes with edits, will now do a final pass: DONE, it is good.
(b) OK only tiny changes.
(c) OK and it is good
(d) OK and it is good, did a few small repairs.

Appendix A. This will be my first pass through this apart from 1991. Very tedious, but it all held together and it is just fine!

Summary**:** I wrote a summary of each chapter for the first time. I am hazy on chapters 7,8,9 and need to proof them and then improve the summaries. We are actually moving forward again!

Sat Feb 9.

I will skip proofs on this proofing run, but will try to check equation number references in proofs.

Question regarding 1.13: Does this say that all Galois fields are commutative under • ?? Well this is trivially true just because GF is a field. Not to worry.

Chapter 1 (21 pages)

equation number continuity check: OK thru (1.45)
(a) OK and very good. A good opening section for the reader.
(b)
1. OK
2. OK
3. OK . Facts have no "fact numbers" in this section.
4. OK and very good. I find that the text is "readable" after being away for a while.
5. OK

(c) Rings and Ideals
1. OK. leave in joking phrases.
2. OK on residue class rings
3. OK, principle ideals
4. OK
5. OK and excellent, shows Z/(n) = Z_n and ties (n) to (f(x)) later to come.
6. OK, added a Maple check on an example
7. OK. I constantly make small edits.

Summary. Reread the summary and see if still seems good. // Well, my summary is short and stays focused on the R/I aspect of Chapter 1. I think this is the way to go, trying to reveal the main thread of the document and filter away as much detail as possible. Details are all made clear in Chapter 1 which

is a very long 21 pages chock full of stuff. I have lots of "words" to help the reader. I am of course the main reader I have in mind, I stand in for other potential readers.

I will not proof this chapter again. It is 100% done. Probably there are typos and someday I might find them.

Chapter 2 (6 pages)

equation number continuity check: OK thru (2.11), this is only a 5 page chapter.
(a) OK
(b) OK, super big fact shows the triple isomorphism
(c) OK, we end with a small list of facts.
Summary: Paragraph is OK, slight edit just now.
This chapter needs no further proofing, it is finis!

Before continuing, I want to eliminate the double appearance of how to multiply two polys. this has not appeared yet, so Chapters 1 and 2 won't be affected by whatever change I make. The first occurrence is at (4.11) and this is where I show full detail. Sums run 0 to m-1 here. The second occurrence is near (8.2) where I use theta functions. // DONE, I leave them both in since they are different.

No! I decided to add Appendix D which does the product for arbitrary upper endpoints. Then I can quote this appendix result in the three places it is needed! // did this, and I have now quoted Appendix D three times. DONE!

Chapter 3 (11 pages)

equation number continuity check: OK thru (3.17)
(a) OK, this took a while, small changes made
(b) OK, repaired a sequencing problem
(c) OK
(d) OK
(e) OK
Summary:

Chapter 4 (16 pages)

equation number continuity check: OK through (4.43) !!
(a) OK after various tunings
(b) OK
(c) OK and very short, base and extension field concepts
(d) OK, this is a monster 9 page section of all facts and proofs, up to Fact 16.
(e) OK
(f) OK. Example showing the two bases.
(g) OK.
Summary: Did some editing, it is already too long so won't add more. This is major chapter.

That is enough proofing for today. I have now proofed 53 of 171 pages, so not even 1/3 done! Maybe do appendices next which have already been "used" before I forget what they were about!

Chapter 5 (23 pages)

equation number continuity check: OK through (5.43)
(a) OK and reads pretty well I think
(b) OK on prim polys and prim elements // MRL furnace back on, Susan!
(c) OK, section of examples, it is very good
(d) OK, totient thing, very good addition.
(e) OK, just fine
(f) OK
(g) OK
(h) OK, made this cyclotomic to be a new section
(i) OK, make this LCM a separate section
Summary: Updated and improved.

Chapter 6 (20 pages)
equation number continuity check: OK through (6.22)
(a) OK, this is a very good review, I think it is well-placed in the paper
(b) OK, lots of examples of enumeration tables
(c) OK. I updated all the Maple stuff to get polys sorted properly.
(d)
1. OK.
2. OK, Maple multiplies out my polynomials and gets the right answers.
3. OK
4. OK
5. OK. These sections show how to do algebra things with Maple.

Summary: did some editing and reordering here. All done

Appendix A (5 pages)
equation number continuity check: there are no equation numbers in this proof.
OK, all done.

Appendix B (5 pages)
equation number check is OK.
I went over this in detail recently. Today I read through and checked equation references.

Appendix D (2 pages)
OK, equations and words. Very short, how to do a(x)b(x).

I will stop here Sunday night Feb 10. The next chapter is a major change of topic.

Resume Monday Feb 11, 2013.

Right now I am going to **swap C↔D appendices** and do all related edits.
1. Edit the two appendices: DONE. Now D = matrices, C = a(x)b(x)
2. Fix all references to appendices. DONE.

Appendix D (6 pages) // the new one on matrices.
equation number continuity check: OK

I did various edits today, this is a very good section. Added information on "secular" and ε tensor.

Chapter 10 (14 pages)

equation number continuity check: OK through (10.41)
(a) OK. This took a long time to get stable!
(b) OK and pretty good. I tried hard to nail things down solidly.
(c) OK, constantly making small edits and additions.
(d) OK, more edits, all in fine shape I think.
Summary: OK, also the four appendix overviews are OK.

I remains to proof Chapters 7,8,9 on codes.

Chapter 7 (17 pages)

equation number continuity check: OK through (7.37)
(a) OK, cleaned up direct sum and direct product idea some more.
(b) OK, all my notation details, took a while, added direct product with outer product.
(c) OK, the parity check matrix H.
(d) OK, has my nice drawing showing the dual code (n,n-k).
(e) OK, the GH=1 proof is a bit hard to follow but leave as is. **Resume Feb 12 Tues**
(f) OK on Feb 12, the linear dependent column stuff got more words added.
(g) OK, and in fact very good. No book I know of shows this level of detail.
(h) OK, very short, syndrome defined.
(i) OK, code history, did some edits here.
Summary: updated a bit, it was not bad to begin with.

Question: d = (d_1, d_2, d_3) and $\mathcal{V} \oplus \mathcal{V} \oplus \mathcal{V}$. Why is this a direct sum and not a direct product? Do I have notes on this? Yes I do, with direct verification, it is OK. I added notes on this right in Ch 7 start.

Bug: My code space pictures make no sense, so we grind to a halt now in our proofing efforts. // OK, this resulted in a new Chapter 7 section (g). Tomorrow I will resume above with section (f).

Chapter 8 (17 pages)

equation number continuity check: OK through (8.35)
intro: OK
(a) OK, a few small edits, returning red regions to black as well.
(b) OK, no real edits
(c) OK, a few edits
(d) OK on CRC, I like it.
(e) OK, an excellent and simple section, the 1 to 1 of cyclic and systematic bases.
(f) OK and excellent, show code is cyclic
(g) OK, a little rocky, ideal (g(x)), not clear where we are headed.

I see there is some confusion about the meaning of poly of degree s. The generator is of degree n-k and will actually have a term x^{n-k} . However, d(x) can be of any degree UP TO k, and then c(x) will be any degree from n-k up to n. This is because c(x) = d(x)g(x) and g(x) has a "hard" degree n-k. I now want to review all my stuff to make sure I have not said this wrong somewhere.

Chapter 3? Nothing really, I do mention A and B as upper limits of a(x) and b(x). A remainder poly always has degree LESS THAN some number. But look at section 3 (d) now. In R/f(x), when we say f(x) has degree m, that is a hard degree. Chap 3 seems completely clean.

Scan for word "remainder" and make sure no bad text. Don't care about Ch 1 which has no polys. Found one violation in Ch 3. This was the only violation in the entire doc.

Now start Chap 8 and make sure things are clean in statements about d(x) and c(x) !!! I refined my definition of degree above (3.1). I am having to do major repairs here!! Just did Fact 2 (8.10). I now say things like d(x) has degree $s \leq k-1$. Fact 3 OK. I have now cleaned up through line (8.20), and I will now resume proofing and repairing.

Ready now to start (h) again, after I failed on the first attempt.

Time to stop. I am drawing chart pictures, things have to be redone in this area near Ch 7 (g). So put that off till tomorrow. // Resuming now 5 AM **Weds Feb 13**.

Question: I have now rewritten section (h) about the standard array. Suppose the incoming bad code word which has n symbols has n bad symbols, so we have an n-symbol error!!! The decoder finds the incoming word in its standard array as a_{ij} and corrects to some c_i. OK, I added text to resolve this.

I am now going to reproof sections (g) and (h) which have been heavily rewritten today.

Chapter 8 (17 pages)

(g) OK, equations numbers and Figure numbers also OK.
(h) first, did equation renumber so that following section (i) can stay as it was.
OK, done proofing h. It is the only offering I have on error correction in this doc.
(i) OK, did some small edits and made a major change: word induced is no longer needed!
(j) OK finally, and the XOR stuff survives another challenge!!

4:30 PM. A lot has happened:

• I changed the m-tuple ordering convention, reversing it from what it was. This required going through the entire document to adjust. Also, all + and • tables had to get changed. It is much better this way.

• I added Section 6 (e) which derives the + and • tables for GF(4) as a sort of extended example, at the end of the section where I say it is easy to do but I never did an example. My tables agree exactly with Rhee p 27. Earlier I quoted the table with no proof, just verified on element!

• I got confused once again about whether or not you can use XOR gate adders in my poly multiplier section. To clear this up, I edited my previous notes above in this edit log.

• After all these things, I now try to finish Chapter 8.

Resume Thurs Feb 14.

Chapter 9 (17 pages)

equation number continuity check: OK through (9.35)

(a) OK, but there is one unresolved issue

(b) OK, I think this is a pretty good section, did some small additions.

(c)

1. OK, not very coherent, about the H matrix for BCH narrow sense
2. OK, on the strange Hamming subset of things.
3. OK and pretty good I think, ties in earlier theorems
4. OK, although based on P&W, this has a lot of my own stuff in it.
5. OK, but see comment below.

Overview: completed on Feb 15

In the RS section, I should comment that we are giving up the benefits described in Section 8 (j) and now we have to really multiply things that need to be multiplied, instead of add or don't. I want now to see some book or web verification that RS codes really need true multipliers. Rhee on page 223 shows a RS encoder in the top of page drawing, and in the text he says $\oplus$ is the XOR adder, but $\otimes$ is the full-bore GF(q) multiplier. Now look in PW for a confirmation of Rhee.

Question: I think I know how to multiply two numbers in Z_{256}. You do the little add and shift business just as in grade school. Why is this true? Because in the mod range n,m < 256, multiplication really is just "regular" multiplication. But the GF(256) table is different. So it is not clear that any kind of add and shift works. You really have to look it up. I just found a Xilinx App note on Galois Field multipliers!

Related question: I have this statement for Z_n

$$\mathbf{a} \bullet \mathbf{b} = \text{Rem}[ab/n]\ \mathbf{1} \qquad \mathbf{a} + \mathbf{b} = \text{Rem}[(a+b)/n]\ \mathbf{1} \tag{1.28}$$

There should be some corresponding statement in the poly world, but I have never written it down. It might say

$$a \bullet b = \text{Rem}[\, a(x)b(x)/f(x)] \qquad a + b = \text{Rem}\,[\,(a(x) + b(x))/f(x)]$$

I really should get this into the doc somewhere if it is true. DONE, I added what was needed to (3.14) !

Feb 15, 2013

I have now completed this very long round of proofing, hundreds of changes were made. Today I read through the TOC and made a few changes. The Summary section is complete. And then I did a Preface section. That word seems better than Overview for this paper. I now have to deal with various cosmetic issues.

1. QED or Q.E.D. ? I decided to use **QED** and put it far to the right.

2. Chapter or Section? All my other documents have Sections. Chapters sounds more like a book, Sections more like a paper. // I will leave it as Chapters, since that is how it started. Nothing wrong with a little variety I guess.

3. Ch or Chapter in references? My references are already cluttered, as in Ch 8 (a) 2, so I want to minimize any extra symbols. So Ch instead of Ch. and instead of Chapter. // Reversed myself. I decided to write out Chapter everywhere, and commonly you will see Chapter 4 (a) 2 as a reference.

4. Added my usual bad links comment.

5. Added all section headers.

Reproof Chapter 9 without reference checks:

Chapter 9

equation number continuity check: OK through (9.35)
(a) OK
(b) OK
(c)
intro OK
1. OK, not sure this theorem is used anywhere.
2. OK
3. OK and very good
4. OK, the modified H code
(d) OK
(e) OK, perhaps a strange section to add, just a personal thing.
Summary section: OK

I am throwing out this comment because it makes no sense to me now:

"The fact that this Hamming subcode exists inside the BCH N=1 code seems to be a quirk of the latter code. The N=1 BCH code for GF(q=p^m) happens to have n-k = m, so there are m rows in its H matrix. This then matches the number of rows in a GF(q=p^m) m-tuple, and these m-tuples are the column vectors of the H_1 matrix which then also has m rows. Both H and H_1 also have n columns. "

I think ALL cyclic codes by (8.1) (b) have n-k = m, the above would be true for any cyclic code using (8.31) for H.

Need a Reed-Solomon reference!!! ****** ??

Chapter 7

(a) (b) (c) (d) all OK
(e) OK
(f) (g) OK
(h) (i) OK

Preface and Summary: OK

Now scan for "red ink" areas and repair as needed.

- near 2.6, got in the GF(4) to Z_4 + and • table comparison as (2.6)

We are ready now for pagination!!!

contents: OK
Preface: OK
Summary: OK and long
Chapter 1: OK thru 28 and DONE, added some page breaks and small adjusts.
Chapter 2: OK thru 33 and DONE.
Chapter 3: OK thru 44, adding a lot of page breaks now, DONE.
Chapter 4: OK thru 59 DONE
Chapter 5: OK thru 81 DONE
Chapter 6: OK thru 101 DONE.
Chapter 7: OK thru 120 DONE
Chapter 8: OK thru 140 DONE
Chapter 9: OK thru 156 DONE
Chapter 10: OK thru 169 DONE.
Appendix A: OK thru 173 DONE
Appendix B: OK thru 176 DONE
Appendix C: OK thru 178 DONE
Appendix D: OK thru 183 DONE
References: OK thru 185 DONE

The last page is p 185.

Enter the Word doc properties as usual, DONE

Lets try a first ever PDF! Started but did not finish! This has happened before.
Tried again and we are there.

Check the document structure in the PDF bookmarks pane:
Ch 2 (c) has leading space -- this is the sole flaw, so put on errata list.

How about the ⊕ and ⊗ symbols? OK and all seem well.

I have started the errata document. First PDF scan looks very very good!! I think we are there!!!

Feb 16, 2013

Proofing in the PDF with errata list building

TOC: DONE, and lots of items to do!

References: DONE, lots to do here as well.

Preface: DONE

Summary: DONE

I found so many things to fix just proofing the above items that I will fix them now and then do a new PDF generation. Takes less than 3 minutes to make a new PDF.

First PDF of Feb 16. Verified a few of the listed errata fixes, then verified that no blank pages. So my first round of errata is finished, ready to start another round.

Chapter 1 easy scan:
(a) OK (b) OK STOP after that.

Well there is no such thing as an easy scan. Proofing this document takes at least a minute per page and that would be 3 solid hours! It is time to let it go I think. I will fix what I found. Surely there are many errors and problems, but I have already spent way too long on this document. At least there is nothing horrible in the first hour of reading a reader will encounter.

I installed a second round of fixes and will now do another PDF cycle, second of Feb 16. DONE.

Time now for a general cleanup, then publish, then push.

Changes for a New Release. Changes made starting June 30, 2013

June 29 Sat

Distractions. I ended up writing a better proof for Galois (5.35) which says that all elements of a conjugate set have the same order. I think my previous proof was OK, but this new one is more interesting and I did a Maple verification.

My question of the day is this: Is there a relationship between the period of h(x) and the order of the conjugate set elements that h(x) is formed from? At first I though those set elements could have different orders, but then I found (5.35) and they all have the same order.

This was a long day of repairs and additions. I showed that elements of a conjugate set do in fact all have the same order. Then I showed that this order is the exactly same thing as the period of the min poly, a proof which took a while. I need to add both these things not to Scrambler but to Galois.

On **June 30** I went through my long list of **Galois errata** and fixed those things up. A few more complicated items remain to be cleared up.

While working on Scrambler, I realized that several new additions should be made to Galois.

I propose now to make the following significant changes to Galois:

• Change the title of section 5 (f) so it is about f(x) *and* about **irreducible classification**. I can do this without upsetting the Chapter 5 equation numbers. This section has only (5.33) and (5.34) as it did before, and one new Figure which will be Fig 5.5 and there are no other figures so that is also OK. **DONE**

• Add a little section about min and prim polys for some GF(p) with p = 2,3,5,7. **DONE**

• Add a whole new section 5 (j) which contains **all my order reversal theorems**. **DONE**

• Then **adjust Fact 12** to refer to this new section. **DONE**

• Then add a new section (k) to Chapter 8 on the topic of " **code word exhaustion by rotation**". This thing is pretty much ready to go. **DONE**

There are more things to do after that, but let's get these things done first.

I now want to **work a bit on Galois Section 6 (d).**

(1) is fine, shows *manual* expansion of a min poly
(2) shows Maple expansion of our favorite example case polynomials
(3) shows Maple going the other way -- factoring an already-expanded polynomial

I might have more to say in this section. This is where I make my incorrect statement.

(4) shows Maple just doing GF(2) multiplications By hand first, then by Maple.
(5) shows Maple doing GF(2) quotients

Now, I want an example of a poly which is not a min poly for my classification chart.

I have **repaired the error in Section 6 (d) 3.** And I will now add a new section 6 to work in my fancier Maple stuff. I added this fancy stuff as Section 6 (d) 6, I think it is pretty good.

I then bit the bullet and wrote a serious Maple program to compute all the factored min polys for any GF(p^m). This took all day and I have long wanted to do it. I installed it as 5 (c) 5, a new little section added onto my hand calculation sections. This I think adds a lot of value to this paper. I said earlier "it would not be hard" and now I have shown that was true.

Now the **Galois errata list is clean except for that CRC item** which I have to track down. I have started a new doc on this. But I see that first I have to do something about my "order and period the same" doc which has other stuff to add to Galois (unless I have already added it and don't remember).

July 3, 2013. Started in on the **CRC stuff** today, collected some very good information, learned that Peterson invented it, but then realized I failed to add some already developed sections to Galois. So I reviewed those and added them and it took the rest of the day. They were

• a **new proof** of (5.35) that elements of conj set have the same order

- the **Order = Period Theorem** for min polys, now Chapter 5 (k)
- Chapter 6 (d) 7 which makes the **connection to the Peterson Weldon Appendix** C.

July 2, 2013 going backwards, forgot to write this down

- added the **Code Word Exhaustion by Rotation** Theorem as Chapter 8 (k)
- Section 5 (d) 6 on how to **classify all irreducible polynomials** using Maple
- Section 5 (d) 5 on my **big Maple program** to do min polys for ANY GF(p^m).
- **Venn diagram** for irreducible polys

I have already started a CRC doc so will continue there, it will be good I think.

July 7, 2013. Yesterday I wrote two **appendices E and F**. One is the **CRC theorems**, the other is the **existence of g(x)** idea. Editing continues unabated. Today I want to get these things linked in, but I still have this question:

Question: **Where do I make use of the x^n - 1 property in the cyclic code stuff?** I asked this question before, but cannot find where

clearing up CRC: not here.
Galois errata: not here
Galois edit log (this doc): not here
finding a new proof for Divisor theorem: not here
order and period same: not here
irreducible and minimum stuff: not here

So I will do it again. The definition is (8.1) and we are in Section 8 (a)

(a) definition and comment that it is optional.
(b) systematic and cyclic bases -- no mention of h(x) or x^n-1
(c) implementation of enc and decoders -- syndrome etc, but x^n-1 not used at all.
(d) CRC: here I now know that x^n-1 with period n is required for double error detection, nada else
(e) how cyclic and systematic are related -- rearrangement, no mention of h(x) or x^n-1
(f) why they are cyclic. Here it IS used.
    The two Math Lemmas do NOT use the h(x) of x^n-1 part of definition, Nothing to do with.
    But in my cyclic proof we DO use $(x^n - 1) = h(x)g(x)$, n can be any integer
(g) The A_n object has x^n-1 in it, but our fact is NOT used in the A_n part.
    the only mention of g(x) here is c(x) = d(x)g(x).

Repair Done: I thought I had shown that (g(x)) was an ideal in A_n without using $(x^n - 1) = h(x)g(x)$, but my proof of Fact 6 (8.21) was WRONG. I fixed everything up after a few hours and now all is well, and this extra requirement IS needed. Continuing along then:

(g) {c(x)} form an *ideal* (g(x)) within A_n only if $(x^n - 1) = h(x)g(x)$. There are no restrictions on n.
    Alternate proof of Fact 5 is OK and since it uses Fact 6, it also needs $(x^n - 1) = h(x)g(x)$
(h) Standard Array stuff. Requires (g(x)) be an ideal, so requires $(x^n - 1) = h(x)g(x)$

(i) Galois-Induced Cyclic codes all require $(x^n - 1) = h(x)g(x)$
All cyclic codes are Galois induced ones.

So I need maybe to strengthen the fact that $(x^n - 1) = h(x)g(x)$ is part of the definition of a cyclic code.

I therefore delete my "optional caveat" earlier inserted into the (8.21) definition.

Conclusion: All the good facts about cyclic codes require $(x^n - 1) = h(x)g(x)$. Only the CRC has some meaning without this property.

Review Appendix E and F. **DONE**.

Make linkage between the cyclic code definition (8.1) and Appendix E on finding g(x): **DONE**.

Make linkage between CRC section and Appendix F on the CRC theorems. **DONE**

I spent a lot of time on this last item, because it is the subject that caused me trouble for the last 5 days or so!

Install Appendix E and F. Both are already spell-checked in their separate files. **DONE**.

July 8, 2013

Wrote the entire Appendix G which has all the little missing pieces of number theory.

July 9, 2013

Reviewed Appendix G, found some errors, added a few more items, also altered the main text to get a clearer statement of mod math explicitly stated.

Next, I want to review those other appendices to get them linked to G and just to check them again.
Appendix E reviewed. Link to Euler's Theorem is adjusted. Seems OK, rather technical.
Appendix F reviewed, made a few changes, all OK. We are still stable.

Linkages to Appendix G.

1. φ(n) is referenced in the main body, fix that all up please. **DONE**.

I have done a lot of shuffling now, and there will be broken cross links.

• I took the big section on order-reversal theorems which was long and boring and put it into an Appendix H which is my last one right now. It used to be Chapter 5 (k) I think. So all those high numbered (5.xx) equation numbers are now (H.xx) numbers, so I have to find them all. The first non-existent is (5.47). So lets search for all and redirect: Did all the (4.4* ones. Now (5.5* done, Now 5.6*. Done.

OK, what's next? Are there any "red" sections left inside Galois doc? The first one was on page 142, here it is:

and note that: $E(x) \equiv C'(x) - C(x) = s(x)$ (8.8c)

The problem is that this is not true of C'(x) is another legal code word. In that case $E(x) \equiv C'(x) - C(x)$ does not vanish, but s(x) does vanish.

OK, this is all fixed up. I have now done several passes through my encoder/decoder section. But why are there no pictures of hardware here? This is page 142.

I show the hardware on page 159, but I show the wrong circuits!!!! I need the one that leaves the remainder in the registers! So fix those right now!

Reviewed section 8 (j) on why want GF(2) coefficients for g(x). I had to replace the hardware pictures because they were the wrong type!! Glad this was caught.

Resume now from page 142 the search for red text. // No more red text!

So now come updates of the Overview sections!

Chapter 1: Nothing to change here. My only change to this whole chapter was to add the mod math equations.
Chapter 2: no change
Chapter 3: no change
Chapter 4: no change
Chapter 5: OK, I added reference to the ending Maple program/
Chapter 6: left it as is, no need to mention new section on WP Appendix C.
Chapter 7: no change
Chapter 8: OK, added rotation by exhaustion note.
Chapter 9 : no change
Appendix A,B,C,D : no change

I now have to add something about the remaining appendices E,F,G,H DONE!

We are now at 229 pages. Pagination comes next.
Perhaps more proofing should be done, I am not sure.
And I have the issue of "phil lucht documents" to ponder.

July 10, 2013

I started off just browsing through, looking at recently written or modified sections. Made various changes. I am now in the CRC section and I see some things I need to do here concerning period of n.

Shortened codes

The actual packet transmitted can have any length $N < n$ and the above theory can still be applied. In this case, the transmitter sends only the N symbols and "in its head only" it sends out N-n zeros to make the

code word have length n. The receiver knows that only N symbols came in (perhaps due to a gap between packets or some other means) so it imagines that the first n-N bits were zeros and acts accordingly. No bandwidth then is wasted sending the imaginary zeros (and of course no errors can occur among them). Usually the zeros are imagined to be at the start of the packet. In such a shortened code, one can, for a fixed n-k, adjust the effective length of the packet to be any convenient N ≤n.

OK, I did a big go-round with the Ethernet example in my CRC section. I had the above blue stuff for a while, but then realized it was not needed. Period of g(x) ≥ n is the new condition, I had to repair Appendix H on this. I think it is all OK, now. I found that I don't how to compute the period of a polynomial other than by Maple brute force which only works for small numbers! This took all day.

I am out of steam on proofing, so I will start paginating. New headings are needed for the new appendices. **DONE**

Adjust eq # positions in new appendices: **DONE**.
So same in newly added sections. **DONE**, not many to do.

Pagination: Luckily each Chapter is independent on this stuff!

TOC: now runs over, not very nice, nothing I can really do about it. **DONE**
Preface: 1 page **DONE**
Summary: It also runs over onto 1/3 page, so be it. **DONE**.
Chapter 1: **DONE**, had to shuffle things due to those new little lemmas etc
Chapter 2: **DONE**, very short chapter, nothing needed here.
Chapter 3: **DONE**, no changes.
Chapter 4: **DONE**, much improved.
Chapter 5: **DONE**, made it better.
Chapter 6: **DONE**, improved.
Chapter 7: **DONE**, no changes.
Chapter 8: **DONE**, changed it.
Chapter 9: **DONE**, no change.
Chapter 10: **DONE**, no change
Appendix A: **DONE**, no change
Appendix B: **DONE**, no change
Appendix C: **DONE**, no change
Appendix D: **DONE**, no change
Appendix E: **DONE**, no change
Appendix F: **DONE**, no change
Appendix G: **DONE**, no change
Appendix H: **DONE**, no change
References: **DONE**

- I still need to ponder how to do references to myself.

- What was it in scrambler doc that caused this major Galois update? Better make sure it is included!

July 11, 2013

I think I have a bad reference somewhere to a GCD theorem, just a dim memory. Is it in those final φ(n) theorems in G? No. I added a theorem and then removed it because it was already there in (4.32), that is the thing I am wondering about, some reference to the thing that I later removed. Let it like.

Adding a paragraph below (5.47) so repaginate Ch 5: **DONE**, had to shrink to Maple code size.

What was the Scrambler issue?

(1) need the code exhaustion by rotation theorem

(2) all conjugate set elements have the same order. In retrospect, this seems reasonable since the min poly will have a period equal to that order. Just added note to that end.

(3) the period = order theorem for a prim poly

So yes, there was plenty of motivation to get these things into Galois doc.

Here is a thing I was worried about but is OK

Fact 13: If monic irreducible f(x) is used to construct a representation of GF(q), then f(x) is a minimum polynomial of GF(q) in that representation. Since all representations of GF(q) are equivalent, f(x) is a minimum polynomial of GF(q). (5.33)

The self-reference question.

I am imagining the year 2042 and I am long gone but my website is still in existence somewhere under the maintenance of some organization or person. That surely won't be xmission.com. So I want to make sure a reader can find my other papers if he happens to be reading one that was picked up by a third party distributor, which I see is a common thing to happen. Thus, my website needs to have some search handle like "Phil Lucht Documents" that I can make sure will lead someone to my paper cache through whatever search engine exists at that time.

The drawback that I don't like is this: If I put this phrase inside a doc, then that phrase is found in the doc itself. Is that good or bad? Here is what I see now after doing this in one of my docs:



The second item is my DNA talk PDF link. I just don't like the way this works. Also it did not pick up the title of that DNA paper. Maybe I should give it a better header.

I have solved the problem. I will put the search handle into in-line graphics just as I did with my email address at the start. That should fix things. Here then is my new reference.

P. Lucht, *Tensor Analysis and Curvilinear Coordinates* (2012, http://user.xmission.com/~rimrock/). This document is segmented into two PDF files, the second containing a set of Appendices. If link is bad, search on "Phil Lucht Documents".

OK, now check all bookmarks of the last PDF: **DONE**, they are all perfect.

Equation sequencing checks for new and modified sections:

Chapter 4 near 4.31: OK
Chapter 5 all: adjust Fig 5.5 position! OK
Chapter 6 OK
Chapter 7 OK
Chap 8 OK
Chap 9 OK
all rest OK too.

Let's standardize the QED usage. **DONE**.

I want to change this paragraph

The wonderfully efficient and dense mathematical notations like $\in\ \forall\ |\ \exists\ \Leftrightarrow$ iff are generally replaced by words. Some well-known theorems are not proved, but those that are proved are proved with a (hopefully) reasonable amount of rigor. Lots of "words" are used to reinforce the various concepts, many examples are provided, and there is constant (perhaps excessive) repetition to grind in definitions and "facts" (Mr. Thomas Gradgrind, schoolmaster, is the character quoted above).

I can't think of any other changes, so I will do another PDF cycle now, July 11. Well, maybe first I will clean up all the files, because I might run into something there.

Files are cleaned up, tiny changes always being made.

Ready now for the release! This update has taken about 12 whole days!!!

****

July 13, 2013

It didn't take long for the release to need replacement. First, some equation numbers and QED's in App G were shifted to the next line. More importantly, for reasons to be explained below, I want to add this Fact to the end of Appendix G and adjust the opening text of App G as well

---

Fact 15: Consider the Diophantine equation ax = by where a,b > 0. Consider the set of solutions (x,y) in which x,y > 0. The solution with the smallest value of x is (x = b/d , y = a/d) where d = GCD(a,b).

Proof: Let N_1, N_2 be the positive integers $N_1 = a/d$, $N_2 = b/d$. From **Fact 1**, $GCD(N_1,N_2) = 1$. Also, we see that $ax = by \Leftrightarrow N_1x = N_2y$. The solutions (x,y) of these two equations are the same, so the smallest-x solution will be the same. We shall now determine the smallest-x solution of $N_1x = N_2y$.

According to **Fact 2** with A = x and B = y, we know, since $GCD(N_1,N_2) = 1$ and $N_1x = N_2y$, that $x/N_2 = y/N_1 = I$, a positive integer. Thus, solutions of $N_1x = N_2y$ are $x = IN_2$ and $y = IN_1$ where I is a positive integer. The smallest-x solution must then be $x = N_2$ and $y = N_1$. This is then also the smallest-x solution of equation ax = by. Thus, the smallest-x solution of ax = by is x = b/d and y = a/d. **QED**

The above edits to Appendix G are now done. **DONE**

Next, I make changes for (4.21) and (4.22) so that my proof of (4.21) is in fact valid (it was not before). I had a Lemma before as (4.22), but it was proven properly. Now (4.22) is just an application of Fact 15 above which is valid. I put this as a separate Lemma (4.22) just so I don't have to adjust all the Chapter 4 equation numbers by deleting 4.22. **DONE**

Lemma: The smallest integer m such that km = nN is $m = n/GCD(k,n)$. (4.22)

Proof: In (G.21) it is shown that, for ax = by, the smallest-x solution is x = b/d where d = GCD(a,b). We apply that here with a = k, x = m, b = n and y = N to find that the smallest-m solution is m = n/d where d = GCD(k,n).

****

Question: Do I have some simple way to compute the order of the elements of a conjugate set and therefore the period of their min poly? Yes, I know it divides q-1, but is there some simple formula for it? It is the order of the cyclic subgroup which any of those α's of the min poly generates. These subgroups are NOT the same as the conjugate set groups, or are they? The number of elements in a conjugate set is the *degree* of m(x), not the *order* of m(x). [Resume here next time]

Well maybe the answer to this question is totally obvious. In the case of m = 4

GF(2^4)

$p_1(x)$	$= (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)$	$= x^4 + x + 1$	10011
$p_7(x)$	$= (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11})$	$= x^4 + x^3 + 1$	11001
$m_3(x)$	$= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)$	$= x^4 + x^3 + x^2 + x + 1$	11111
$m_5(x)$	$= (x - \alpha^5)(x - \alpha^{10})$	$= x^2 + x + 1$	111

(6.21)

We know that $\alpha^{15} = 1$ for a prim element α. Look at p_7. What is the smallest n such that $(\alpha^7)^n = 1$? That means 7n mod 15 = 0, find smallest n. It has to be n = 1,3 or 5. So 1 does not work, and 3 does not work. Then 35 mod 15 = 5 and that does not work either. But of course 15 does work. and it is prim.

Next, try m3. 3n mod 15 = 1 has solution m = 5.

Next try m5: 5n mod 15 = 1 has solution m = 3.

So here is the general solution. Let a be the first power. the rule is an mod p^m-1 = 0. Why have I never stated that anywhere in Galois doc? Again, solve an mod q-1 = 0.

I need to get this Fact inserted somewhere:

order(α^k) = (q-1)/GCD(k,q-1).

I have it in a different form in Fact 6 (4.21) and I just want to apply that fact to all of GF(q)-0. How about this idea: Here is how Fact 12 stands right now

Fact 12: A power α^k of a known primitive element α of GF(q) is itself a primitive element if and only if GCD(k,q-1) = 1. (4.32)

Here is a new version

Fact 12: If α is a primitive element of GF(q) then :

(a) order of (α^k) = (q-1)/GCD(k,q-1)

(b) if GCD(k,q-1) = 1, then α^k is also a primitive element of GF(q)

(c) if GCD(k,q-1) ≠ 1, then α^k is not primitive element of GF(q) (4.32)

Proof: Part (a) is just Fact 6 (4.21) applied to the cyclic group {GF(q)-1, • }. For Parts (b) and (c):

If GCD(k,q-1) = 1, then (a) says order of (α^k) = (q-1) and by the definition of a primitive element of GF(q) we conclude that α^k is primitive. Conversely:

If GCD(k,q-1) ≠ 1, then GCD(k,q-1) = N > 1, and order of α^k = (q-1)/N, so in this case α^k is not a primitive element.

I just installed it, **DONE .** Luckily there was no Chapter 4 pagination effect, since page 58 ended already with a next page deal.

Next, I updated the Chapter 5 (k) Maple program so it also displays order = period. Also update all the examples run with this program so that number shows. **DONE**

Next, I had to modify Section to explicitly show the defining prim poly for each of my cases. Otherwise reader has no idea how the subs command is working. **DONE**

This requires that I repaginate Chapter 6. **DONE**

Tonight I will do a new release but let's hold for the moment and make sure my scrambler problems are solved.

Aug 31, 2013. Fixed two items and did a whole new release, see errata list.