Harold Edwards Fermat's last theorem

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: March 11, 2018)

Abstract

Page 8, Problem 1. We need to find p and q, what we have is

$$p^2 - q^2 = 4961$$
$$2pq = 6480$$
$$p^2 + q^2 = 8161$$

the easiest thing to do is to add $(p^2 - q^2) + (p^2 + q^2)$, but let's be a masochist and do $p = 3240/q$ and substitute it to $p^2 + q^2 = 8161$

$$\frac{3240^2}{q^2} + q^2 = 8161$$
$$3240^2 + q^4 = 8161q^2$$

using the quadratic formula

$$q^2 = \frac{8161 \pm \sqrt{8161^2 - 4 \cdot 3240^2}}{2}$$
$$= \frac{8161 \pm 4961}{2}$$

so q^2 is either $1600 \to q = 40$ or $6561 \to q = 81$. This gives us both answers, if $q = 40$ then $p = 81$ and if $q = 81$ then $p = 40$.

Page 8, Problem 2. Extend the Pythagorean table to $p = 12$, no derivation needed, just having some fun calculating numbers, been a long time since I calculated numbers by hand, see Table. I for result.

Page 8, Problem 3. Show that if $d^2|z^2$ then $d|z$, start with $\gcd(d, z) = c$

$$d^2k = z^2$$
$$c^2D^2k = c^2Z^2$$
$$D^2k = Z^2$$

we know that $\gcd(D, Z) = 1$ and so $\gcd(D^2, Z^2) = 1$, since $k|Z^2$, if $\gcd(D^2, k) > 1$ then $\gcd(D^2, Z^2) > 1$ as well, therefore $\gcd(D^2, k) = 1$, this means that $k = K^2$ by our assumption that if $vw = u^2$ and v and w are co-prime then both v and w are squares.

Substituting $k = K^2$ back into our first equation

$$d^2K^2 = z^2$$
$$\to dK = z$$

TABLE I: Pythagorean triples. Proudly calculated by hand (I only made two mistakes).

p	q	x	y	z		p	q	x	y	z
9	2	77	36	85		11	4	105	88	137
9	4	65	72	97		11	6	85	132	157
9	6	45	108	117		11	8	57	176	185
9	8	17	144	145		11	10	21	220	221
10	1	99	20	101		12	1	143	24	145
10	3	91	60	109		12	3	135	72	153
10	5	75	100	125		12	5	119	120	169
10	7	51	140	149		12	7	95	168	193
10	9	19	180	181		12	9	63	216	225
11	2	117	44	125		12	11	23	264	265

thus $d|z$ although I'm not sure about this particular line of reasoning, since $\gcd(D^2, Z^2) = 1$ and $D^2|Z^2$ then $D^2 = 1$ and we immediately get $k = Z^2$ and we don't need our assumption about $vw = u^2$ at all. But I'm not sure how else to show that $\gcd(D^2, k) = 1$ except by showing that $\gcd(D^2, Z^2) = 1$.

Now, the one step I stil need to prove, is that $\gcd(D, Z) = 1$ means $\gcd(D^2, Z^2) = 1$, again, without using the fundamental theorem. What I need is Bezout, assume that $\gcd(D^2, Z^2) = g > 1$ then Bezout tells us that

$$D^2a + Z^2b = g$$

but from $\gcd(D, Z) = 1$ we also get

$$DA + ZB = 1$$
$$\rightarrow DgA + ZgB = g$$

Now there might be some other numbers such that

$$DM + ZN = g$$

but this means either that $\gcd(M,N) = g$ or $\gcd(M,N) = y|g$, let's dicuss the latter first

$$DyM' + ZyN' = yg'$$
$$DM' + ZN' = g'$$

with $\gcd(M',N') = 1$ but this means that $\gcd(D,Z) = g'$, the only way this works is that $g' = 1$ and $\gcd(M,N) = g$, but if this is the case then

$$DM' + ZN' = 1$$

but Bezout also tells us that all solutions to $DA' + ZB' = 1$ are of the form see ent.pdf Problem 2.5

$$A' = A + lD$$
$$B' = B - lD$$

Equating the two Bezouts $g = D^2a + Z^2b = DgA' + ZgB'$

$$\rightarrow gA' = gA + glD = Da$$
$$\rightarrow gB' = gB - glZ = Zb$$

Now, equating the two Bezouts again

$$D^2a + Z^2b = DgA + ZgB$$
$$D(Da - gA) = Z(gB - Zb)$$
$$\rightarrow D(glD) = Z(glZ)$$
$$D^2 = Z^2$$

which is a contradiction, therefore if $\gcd(D,Z) = 1$ then $\gcd(D^2,Z^2) = 1$ as well. The above proof is easily generalizable to $\gcd(D^n,Z^m)$

$$\rightarrow gA' = gA + glD = D^{n-1}a$$
$$\rightarrow gB' = gB - glZ = Z^{m-1}b$$

Now, equating the two Bezouts again

$$D^n a + Z^m b = DgA + ZgB$$
$$D(D^{n-1}a - gA) = Z(gB - Z^{m-1}b)$$
$$\rightarrow D(glD) = Z(glZ)$$
$$D^2 = Z^2$$

Page 14, Problem 1. Prove that if Ad^2 is a square then A is a square, using the result from previous Problem, say $Ad^2 = z^2$ since $d^2|z^2$ this also means that $d|z$ so we can write $z = dk$, therefore

$$Ad^2 = z^2 = d^2k^2$$
$$A = k^2$$

and we are done.

Page 14, Problem 2. Show that $x^4 - y^4 = z^2$ has no non-zero integer solutions. One thing we should not do is to blindly apply the Pythagorean formula $(m^2-n^2, 2mn, m^2+n^2)$ over and over again, what we should do is follow what was done in the preceding section.

In that section we have p, q, and $p^2 - q^2$ are all squares due to $t^2 = pq(p^2 - q^2)$ so if we designate

$$p = x^2$$
$$q = y^2$$
$$p^2 - q^2 = z^2$$
$$\rightarrow x^4 - y^4 = z^2$$

and we have our current problem. Following what was done in the book

$$z^2 = p^2 - q^2$$
$$= (p - q)(p + q)$$

since p and q are co-prime so are $p - q$ and $p + q$. From $x^4 - y^4 = z^2$ we know that x and thus p is odd but here we can have y even or odd, for simplicity let's start with y and thus q even so that we have the case in the book, so

$$p + q = r^2 \qquad\qquad p - q = s^2$$

with both r and s odd and co-prime and

$$u = \frac{r-s}{2} \qquad\qquad v = \frac{r+s}{2}$$

with u and v integers and co-prime and so

$$uv = \frac{r^2-s^2}{4} = \frac{(p+q)-(p-q)}{4} = \frac{q}{2} = \frac{y^2}{2}$$

since uv integer $y^2/2$ must also be an integer, thus $y = 2k$, $y^2/2 = 2k^2$ therefore

$$\begin{aligned} \frac{uv}{2} &= \frac{y^2}{4} = k^2 \\ \rightarrow uv &= 2k^2 \end{aligned}$$

since u and v are co-prime this means that one of them is even and the other odd, let's take u odd and $v = 2v'$ even, then $u(2v') = 2k^2$ and therefore

$$u = U^2 \qquad\qquad v = 2V^2$$

since u and v are coprime. Thus

$$r = u + v = U^2 + 2V^2$$

and

$$\begin{aligned} u^2 + v^2 &= \frac{(r-s)^2 + (r+s)^2}{4} \\ &= \frac{2r^2 + 2s^2}{4} = \frac{r^2+s^2}{2} \\ &= \frac{(p+q)+(p-q)}{2} = \frac{2p}{2} \\ &= p \\ u^2 + v^2 &= x^2 \end{aligned}$$

Thus we have a primitive triple u, v, x (because u, v are co-prime), thus we have $P^2 - Q^2, 2PQ, P^2 + Q^2$ (note that above we have designated u as the odd one) and so

$$\frac{uv}{2} = k^2 = (P^2 - Q^2)PQ$$

so we have the same situation as $t^2 = pq(p^2 - q^2)$ but $uv/2 = q/4 < t^2$ and our infinite descent begins.

The above was when q even such that $p-q$ and $p+q$ are odd. Now we deal with the case of q odd such that $p-q=2r^2$ and $p+q=2s^2$ are both even, this is because now $p-q$ and $p+q$ are no longer co-prime so we cannot follow the same steps above.

What we have is (from the pythagorean triple formula)

$$p=x^2=m^2+n^2$$
$$q=y^2=m^2-n^2$$

thus we can use them directly, m^2 plays the role of p and n^2 play the role of q as they are already co-prime and of opposite parities and of course x plays the role of $p+q$ and y, $p-q$. Thus in this case

$$u=\frac{x-y}{2} \qquad\qquad v=\frac{x+y}{2}$$

Thus, just like above

$$uv=\frac{x^2-y^2}{4}=\frac{n^2}{2} \qquad\qquad u=U^2 \qquad v=2V^2$$

and therefore

$$u^2+v^2=m^2$$

Thus we have our infinite descent all over again.

Page 19, Problem 1. Prove that if x^2+y^2 is an odd prime then it is of the form $4n+1$. We can go about it by showing that -1 is a quadratic residue or we can just do mods.

Since x^2+y^2 is odd then one of them is odd and the other even, doing mod 4, then one of them is 1 mod 4 and the other 0 mod 4.

Page 19, Problem 2. Prove that if x^2+3y^2 is an odd prime other than 3 then it is of the form $6n+1$. Again, without quadratic residue stuff, just do mods.

Since x^2+3y^2 is odd then one of them is odd and the other even. If y is even then x must be odd, let's list the possibilities. This also means that $3y^2\equiv 0 \mod 6$, note also that since x is odd it can only be of the form $1,5 \mod 6$

$$x^2\equiv 1 \mod 6 \rightarrow x^2+3y^2\equiv 1 \mod 6$$

so the only possibility is $1 \mod 6$. Let's check the other possibility, x is even, y odd. An even number (mod 6) can only be of the form $2, 4 \mod 6$ therefore $x^2 \equiv 4 \mod 6$, y can only be $1, 5 \mod 6$, so $y^2 \equiv 1 \mod 6$, therefore $x^2 + 3y^2 \equiv 1 \mod 6$.

Page 19, Problem 3. Show that if $x^2 + 2y^2$ is an odd prime then it is of the form $8n + 1$ or $8n + 3$. Again, without quadratic residue stuff, just do mods.

Let's do mod 8 as the problem suggested, x can't be even since $2y^2$ is always even, so x must be odd, this means $x \equiv 1, 3, 5, 7 \mod 8$ and $x^2 \equiv 1 \mod 8$. On the other hand y can be anything, listing all the squares mod 8 we get $2y^2 \equiv 0, 2 \mod 8$, thus $x^2 + 2y^2 \equiv 1, 3 \mod 8$.

Page 19, Problem 4. Girard's condition says that a number is a sum of two squares if it's (1) a square, (2) prime of the form $4n + 1$, (3) the number 2 or (4) the product of the previous three. If we divide out the largest square a contains, then the quotient no longer contains any square (and this is the key which can be easily seen by expanding the number in terms of its primal constituents), so by Girard's condition it must be a product of two's and odd primes of the form $4n + 1$. Once we divide out all factors of 2 out of the quotient, what we have left is just a product of odd primes, but we know that odd primes can only be of the form $4n + 1$ or $4n + 3$, thus if there is an odd prime of the form $4n + 3$, the number fails to obey Girard's condition and cannot be written in the form $x^2 + y^2$even if one of them is 0 (again since we already divided out the largest square the quotient no longer contains any square factor).

Page 19, Problem 5. Show that Girard's condition implies that there are no *rational* numbers x, y such that $x^2 + y^2 = 15$. Let's express $x = a/b, y = c/d$ then if there are rational solutions

$$\frac{a^2}{b^2} + \frac{c^2}{d^2} = 15$$
$$(ad)^2 + (bc)^2 = 15(cd)^2$$

From the previous Problem, if we divide out th largest square out of $15(cd)^2$ we just got 15 and 15 contains $3 = 4 \cdot 0 + 3$ and therefore there must not be any rational solution.

Page 19, Problem 6. Prove that a product of two numbers of the form $x^2 + 5y^2$ is

TABLE II: Searching for primal constituent of $2^{37}-1$.

p	$2^8 \mod p$	$2^{16} \mod p$	$2^{32} \mod p$	$2^{37} \mod p$
149	107	125	129	105
223	33	197	7	1

also of this form.

$$\begin{aligned}(x^2+5y^2)(w^2+5z^2) &= (xw)^2+5(xz)^2+5(yw)^2+25(yz)^2\\ &= [(xw)^2+(5yz)^2]+5[(xz)^2+(yw)^2]\\ &= [(xw)-(5yz)]^2+2\cdot 5(xwyz)+5[(xz)^2+(yw)^2]\\ &= [(xw)-(5yz)]^2+5[(xz)^2+2(xzyw)+(yw)^2]\\ &= [(xw)-(5yz)]^2+5[(xz)+(yw)]^2\end{aligned}$$

Had we chosen $[(xw)^2+(5yz)^2] \to [(xw)+(5yz)]^2$ we would've gotten $[(xw)+(5yz)]^2 + 5[(xz)-(yw)]^2$ as a final result.

Page 25, Problem 1. Prove that $2^{37}-1$ is not prime, from what's described in the book, the only prime that can divide this number must be of the form $p=37n+1$ because $2^{37} \equiv 1 \mod p$, thus $37|p-1$. But what we need to do to check is to calculate the residue of $2^{37} \mod p$. we don't need the order d of 2 mod p.

An easier way to calculate $2^{37} \mod p$, is to first calculate $2 \mod p$, then $2^2 \mod p$, followed by $(2^2)^2 \mod p$, etc, until we reach $2^{37} \mod p$. This is because we just need to square our previous result and then take the mod p of that square, this way we are only doing roughly $\log_2 37 \sim 5$ operations for every possible prime factor of $2^{37}-1$. But before we start, the smallest prime of the form $37n+1$ is 149, so we only need to start calculating from $2^8 \mod p$ and for $2^{37} \mod p$ we just multiply $2^{32} \mod p$ and $2^5 \mod p$. Let's start, see Table. II. It's actually quite funny that the second prime you try already divides $2^{37}-1$:) So $2^{37}-1 = 223 \times 616318177$. As a trivia, there are 885 primes of the form $37n+1$ that are $\leq \lfloor\sqrt{2^{37}-1}\rfloor$.

Page 25, Problem 2. If $p=4n+3$ divides x^2+y^2 then

$$(x^2)^{2n+1}+(y^2)^{2n+1} = \left[(x^2)+(y^2)\right]\left[(x^2)^{2n}-(x^2)^{2n-1}(y^2)+(x^2)^{2n-2}(y^2)^2\cdots+(y^2)^{2n}\right]$$

and hence $p|(x^2)^{2n+1} + (y^2)^{2n+1}$ as well. But

$$(x^2)^{2n+1} = x^{4n+2} = x^{p-1}$$

and so if $p \nmid x$ and $p \nmid y$ then because $p|x^{p-1} - 1$ and $p|y^{p-1} - 1$ we have

$$\begin{aligned}(x^2)^{2n+1} + (y^2)^{2n+1} &= (x^{p-1} - 1) + (y^{p-1} - 1) + 2 \\ &= pm_x + pm_y + 2 \\ &= pm_{xy} + 2\end{aligned}$$

therefore we have a contradiction as now p no longer divides $(x^2)^{2n+1} + (y^2)^{2n+1}$ as it differs from a multiple of p by 2. But if one of them, either x or y is divisible by p then (for simplicity let's assume it's x)

$$\begin{aligned}(x^2)^{2n+1} + (y^2)^{2n+1} &= pm_x + (y^{p-1} - 1) + 1 \\ &= pm_x + pm_y + 1 \\ &= pm_{xy} + 1\end{aligned}$$

and this time it differs from a multiple of p by 1.

Page 33, Problem 2. This is quite a fun one to do, let's do the one for $A = 13$, we start with

$$1^2 - A \cdot 0^2 = 1$$

multiplying it with $r^2 - A = s$ we get

$$r^2 - A(1 + r)^2 = 1 \cdot s$$

here $k = 1$, so now we need to find an r such that $r^2 < A$ but $r^2 - A$ is a negative number, here since $k = 1$ we do not need to care if $k|(1 + r)$ or not. The answer is $r = 3$ such that $s = r^2 - A = -4$ and our next equation is

$$3^2 - A \cdot 1^2 = -4$$

multiplying it by $r^2 - A = s$ we get

$$(3r + A)^2 - A(3 + r)^2 = -4 \cdot s$$

but now we need to make sure $k = -4$ divides $(3 + r)$, an r that works is $r = 1$ this way $r^2 < 13$ and $r^2 - A = -12$ is negative and so we get

$$4^2 - A \cdot 1^2 = 3$$

next, multiplying it with $r^2 - A = s$ again

$$(4r + A)^2 - A(4 + r)^2 = 3 \cdot s$$

here $k = 3$, to make sure $3|(4 + r)$ and since $r^2 < 13$ we get $r = 2$ and thus

$$7^2 - A \cdot 2^2 = -3$$

and I got tired after this :) so the s we recovered so far are $1, -4, 3, -3, \ldots$

Page 33, Problem 3. The first part is straightforward, since $p^2 - Aq^2 = k$ and $P^2 - AQ^2 = K$ with $P = (pr + qA)/|k|$ and $Q = (p + qr)/|k|$

$$\begin{aligned} pQ &= \frac{p^2 + pqr}{|k|} \\ Pq &= \frac{pqr + q^2A}{|k|} \\ \rightarrow pQ - Pq &= \frac{p^2 - Aq^2}{|k|} \\ &= \pm 1 \end{aligned}$$

as $|k| = |p^2 - Aq^2|$ by definition. Now for the more fun part, since $pQ - Pq = \pm 1$, Bezout tells us that $\gcd(Q, P) = 1$, but from $P^2 - AQ^2 = K$, if $\gcd(Q, K) > 1$ then it will also divide P and vice versa, therefore these three are co-prime.

We need this for the next step, we want a new number R such that $QR + P$ is divisible by K or in other words

$$\begin{aligned} QR + P &\equiv 0 \mod K \\ R &\equiv Q^{-1}(-P) \mod K \end{aligned}$$

we are guaranteed to have such a Q^{-1} because $\gcd(Q, K) = 1$ and the final step is also straightforward, say

$$\begin{aligned} W \equiv QA + PR &\equiv QA + P(Q^{-1}(-P)) \mod K \\ W &\equiv QA - Q^{-1}P^2 \mod K \\ QW &\equiv Q^2A - P^2 \equiv 0 \mod K \end{aligned}$$

and by definition $K|Q^2A-P^2$ but since $\gcd(Q,K)=1$ this means that $W \equiv QA+PR \equiv 0 \mod K$ and we are done.

Page 34, Problem 4. Show that if r and R are the values of r which precede and follow the line $P^2 - AQ^2 = K$ then $r + R$ is divisible by K. [$P - rQ$ is divisible by K.] Note that this vastly simplifies the determination of R at each step.

Again $P = (pr + qA)/|k|$ and $Q = (p + qr)/|k|$, also $r^2 - A = s$

$$\begin{aligned} P - rQ &= \frac{(pr + qA) - r(p + qr)}{|k|} \\ &= \frac{q(A - r^2)}{|k|} \\ &= \frac{q(-s)}{|k|}, \qquad K = \frac{s}{k} \\ &= -\text{sgn}(k)qK \end{aligned}$$

so $P - rQ$ is divisible by K. Or in other words

$$\begin{aligned} P - rQ &\equiv 0 \mod K \\ r &\equiv Q^{-1}P \mod K \end{aligned}$$

from our previous problem we have $R = -Q^{-1}P \mod K$, thus

$$\begin{aligned} R + r &\equiv -Q^{-1}P + Q^{-1}P \mod K \\ &\equiv 0 \mod K \end{aligned}$$

as required :)

Page 34, Problem 5. Note that the simplification of Exercise 4 makes it possible to compute the sequence of k's and r's without ever computing any p's and q's. For example, show that the cyclic method in Fermat's case $A = 149$ in which lines 1 and 2 are $1^2 - 149 \cdot 0^2 = 1$ and $12^2 - 149 \cdot 1 = -5$, respectively, will arrive at a solution $p^2 - 149q^2 = 1$ on line 15. (Do not compute the solution.) Show that the English method will arrive at a solution on line 19.

What the problem is saying is that, find R and then K and repeat the process until you get $K = 1$ which means we get the final solution. For example, using the Indian cyclic method for the above, we initially had $1^2 - A \cdot 0^2 = 1$, to get to line 2 we choose $r = 12$ and $s = -5$, generating $K = ks/k^2 = 1 \cdot -5/1^2 = -5$.

We now need to get the next R, from Problem 4 we know that $K|r+R$, $-5|12+R$, the first R to try would be $R = 3$, but this gives $R^2 - 149 = s = -140$, in the Indian cyclic method we want to minimize the absolute value of s, so we try the next possible value for $R = 8$, this generates $s = -85$, we keep trying, until we found that the minimum $s = 20$ is generated by $R = 13$. The new K is then given by the new s divided by the old K, $K = 20/-5 = -4$. And so on, this is perfect for a python script :) so here they are, this script is the full script including solutions to Problem 5, 6, 7 and 8.

```
# it builds solution starting from line 1
def SolvePell(A=149, English=False, Shortcut=True):

    # cosmetics only
    output_string = "line:{0:3d} r:{1:3d} s:{2:4d} K:{3:3d} P:{4:<17d} Q:{5:<11d}"

    # try to start from line 1
    line = 1
    r = 0
    K = 1**2 - A*0

    # This is for Problem 6, since I'm already writing a script
    # let's use it instead of multiplying matrices
    kK = [0, K]
    P = [0, 1]
    Q = [0, 0]

    # print line 1, the loop below will generate line 2 and above
    # here r and s doesn't make sense since we had nowhere to come from
    print output_string.format(line, r, 0, K, 1, 0)

    while kK[0] == 0 or K <> 1:

        # min_s is to hold the current possible minimum of s
        # has to be reset every time we search for the next K,
        # this is only for the Indian method
        min_s = float('inf')

        # next_R is a dummy variable to contain possible R
        next_R = r

        while True:

            # make sure next_R is different from r
            next_R += 1
            # this loop is here to find R such that r + R is divisible by K
            while next_R % abs(K) <> 0:
                next_R += 1

            R = next_R - r
            next_s = R**2 - A

            # using the Indian cyclic method we want R that minimizes
            # abs(s), so I created this min_s to hold the current min for s
            # produced by the current R (next_R)
```

```
# they way I know that I've got the minimum s is if the next s
# is bigger than the previous one, this way I need to keep
# the previous s and previous R

# for the English method we want to make R as large as possible
# while maintaining next_s to be negative, thus we stop once we get
# a positive or zero next_s

if English == True:
    if next_s < 0:
        prev_s = next_s
        prev_r = R
        continue
else:
    if abs(next_s) < min_s:
        min_s = abs(next_s)
        prev_s = next_s
        prev_r = R
        continue

# Calculate next P and Q, for the first line we cannot use
# the matrix method since there is only one line the matrix
# method requires two
if line >= 2:
    n = (r + prev_r)/abs(K)
    sgn = kK[0]*kK[1]/(abs(kK[0])*abs(kK[1]))

    new_P = n*P[1] - sgn*P[0]
    new_Q = n*Q[1] - sgn*Q[0]
else:
    new_P = prev_r
    new_Q = 1

# now update these values to the new ones
r = prev_r
K = prev_s/K
s = prev_s

kK[0] = kK[1]
kK[1] = K
P[0] = P[1]
P[1] = new_P
Q[0] = Q[1]
Q[1] = new_Q

line += 1

# This is the short cut defined in Problem 7, if two consecutive
# k's are the same magnitude we can multiply the results together
# and divide the new P and Q by k^2 to get p^2 - Aq^2 = \pm 1
# if it's minus one we need to multiply it again to get the final result

if Shortcut == True and abs(kK[1]) == abs(kK[0]):
    # but before preceding, show the twin k's to user first :)
    print output_string.format(line, r, s, K, new_P, new_Q)

    new_P = P[0]*P[1] + A*Q[0]*Q[1]
    new_Q = Q[0]*P[1] + P[0]*Q[1]
    new_K = new_P**2 - A*(new_Q**2)
```

```
            new_K = new_K/(abs(kK[1])**2)

            if new_K == -1:
                new_P, new_Q = (new_P*new_P + A*new_Q*new_Q)/(abs(kK[1])**2),\
                               (2*new_P*new_Q)/(abs(kK[1])**2)
                new_K = new_P**2 - A*(new_Q**2)

            # make sure the outer loop stop
            K = new_K

            print "Final line: K:{0:3d} P:{1:<12d} Q:{2:<11d}"\
                  .format(K, new_P, new_Q)
            break


        print output_string.format(line, r, s, K, new_P, new_Q)
        break
```

with the output

```
line:  1 r:  0 s:   0 K:  1 P:1                Q:0
line:  2 r: 12 s:  -5 K: -5 P:12               Q:1
line:  3 r: 13 s:  20 K: -4 P:61               Q:5
line:  4 r: 11 s: -28 K:  7 P:354              Q:29
line:  5 r: 10 s: -49 K: -7 P:1123             Q:92
line:  6 r: 11 s: -28 K:  4 P:3723             Q:305
line:  7 r: 13 s:  20 K:  5 P:23461            Q:1922
line:  8 r: 12 s:  -5 K: -1 P:113582           Q:9305
line:  9 r: 12 s:  -5 K:  5 P:2749429          Q:225242
line: 10 r: 13 s:  20 K:  4 P:13860727         Q:1135515
line: 11 r: 11 s: -28 K: -7 P:80414933         Q:6587848
line: 12 r: 10 s: -49 K:  7 P:255105526        Q:20899059
line: 13 r: 11 s: -28 K: -4 P:845731511        Q:69285025
line: 14 r: 13 s:  20 K: -5 P:5329494592       Q:436609209
line: 15 r: 12 s:  -5 K:  1 P:25801741449      Q:2113761020
```

so we see that the Indian cyclic method found the solution on line 15. And for the English method,

```
line:  1 r:  0 s:   0 K:  1 P:1                Q:0
line:  2 r: 12 s:  -5 K: -5 P:12               Q:1
line:  3 r:  8 s: -85 K: 17 P:49               Q:4
line:  4 r:  9 s: -68 K: -4 P:61               Q:5
line:  5 r: 11 s: -28 K:  7 P:354              Q:29
line:  6 r: 10 s: -49 K: -7 P:1123             Q:92
line:  7 r: 11 s: -28 K:  4 P:3723             Q:305
line:  8 r:  9 s: -68 K:-17 P:19738            Q:1617
line:  9 r:  8 s: -85 K:  5 P:23461            Q:1922
line: 10 r: 12 s:  -5 K: -1 P:113582           Q:9305
line: 11 r: 12 s:  -5 K:  5 P:2749429          Q:225242
line: 12 r:  8 s: -85 K:-17 P:11111298         Q:910273
line: 13 r:  9 s: -68 K:  4 P:13860727         Q:1135515
line: 14 r: 11 s: -28 K: -7 P:80414933         Q:6587848
line: 15 r: 10 s: -49 K:  7 P:255105526        Q:20899059
line: 16 r: 11 s: -28 K: -4 P:845731511        Q:69285025
line: 17 r:  9 s: -68 K: 17 P:4483763081       Q:367324184
line: 18 r:  8 s: -85 K: -5 P:5329494592       Q:436609209
line: 19 r: 12 s:  -5 K:  1 P:25801741449      Q:2113761020
```

so we see that the English method found the solution on line 19.

Page 34, Problem 6. Here we want to calculate the p's and q's (since they are what we really want). We have three successive lines, let's call them line 1,2,3, $p^2 - Aq^2 = k$, $P^2 - AQ^2 = K$, $\mathcal{P}^2 - A\mathcal{Q}^2 = \mathcal{K}$, and we have r going from line $1 \to 2$ and R to go from line $2 \to 3$.

We need to show that

$$\mathcal{P} = nP \pm p \qquad\qquad \mathcal{Q} = nQ \pm q$$

where n is given by $r + R = n|K|$ and we get plus sign if $kK < 0$ and minus sign for $kK > 0$.

First thing we need is

$$\begin{aligned} Pr - QA &= \frac{(pr + qA)r - (p + qr)A}{|k|} \\ &= \frac{p(r^2 - A)}{|k|} \\ &= \frac{ps}{|k|}, \qquad K = \frac{s}{k} \\ &= \mathrm{sgn}(k)pK \end{aligned}$$

where $\mathrm{sgn}(k)$ is the sign of k, whether it's plus or minus, we then put this into

$$\begin{aligned} \mathcal{P} &= \frac{PR + QA}{|K|} \\ &= \frac{P(R + r) - Pr + QA}{|K|} \\ &= \frac{Pn|K| - \mathrm{sgn}(k)pK}{|K|} \\ &= Pn - \mathrm{sgn}(k)\mathrm{sgn}(K)p \end{aligned}$$

For $\mathcal{Q}$ we need the following

$$\begin{aligned} P - Qr &= \frac{(pr + qA) - (p + qr)r}{|k|} \\ &= \frac{q(A - r^2)}{|k|} \\ &= \frac{q(-s)}{|k|}, \qquad K = \frac{s}{k} \\ &= -\mathrm{sgn}(k)qK \end{aligned}$$

putting this into the definition of $\mathcal{Q}$

$$\begin{aligned}\mathcal{Q} &= \frac{P + QR}{|K|} \\ &= \frac{P - Qr + Q(R + r)}{|K|} \\ &= \frac{-\text{sgn}(k)qK + Qn|K|}{|K|} \\ &= Qn - \text{sgn}(k)\text{sgn}(K)q\end{aligned}$$

as for the actual computation, you can see them from the preceding Problem, the output of the Python script provides everything :) I generally dislike the matrix multiplication and prefer the manual computation as in the script because even with matrices we still need to find out the sign of kK and this needs to be fixed by hand in the matrices.

Page 34, Problem 7. We need to show that if two consecutive k's have the same absolute values we have $pP + AqQ$ and $pQ + qP$ both divisible by k.

Let's list the facts we've gathered so far, in each line, from Problem 3, we know that $\gcd(q, p) = 1$, $\gcd(q, k) = 1$, and since $p^2 - Aq^2 = k$, this means that $\gcd(p, k) = 1$. Another thing is that from Problem 3 we also saw $r \equiv -q^{-1}p \mod k$.

From previous two problems we know that $P - Qr \equiv 0 \mod K$ but here $K = \pm k$, thus $P - Qr \equiv 0 \mod k$ as well. Thus

$$\begin{aligned}P - Qr &\equiv 0 \mod k \\ P - Q(-q^{-1}p) &\equiv 0 \mod k \\ qP + Qp &\equiv 0 \mod k\end{aligned}$$

where we multiply both sides with q to get to the last line. This is the second assertion in this problem we need to prove.

The first one is $pP + AqQ$, I think we should be able to get this from this relation from previous Problem, $Pr - QA \equiv 0 \mod K$ and since $K = \pm k$ this is also $Pr - QA \equiv 0 \mod k$

$$\begin{aligned}Pr - QA &\equiv 0 \mod k \\ P(-q^{-1}p) - QA &\equiv 0 \mod k \\ pP + qQA &\equiv 0 \mod k\end{aligned}$$

where we multiply both sides with $-q$ to get to the last line. And this is the first assertion we needed. And as for the actual computation, you can see them from Problem 5 above, the output of the Python script provides everything :)

Page 34, Problem 8. Here I will just use my Python script :) so we can compare the English method to the Indian cyclic method. For $A = 109$, the Indian cyclic method found the result on line 23 (with the shortcut we would've stopped on line 7), the English method found the result on line 31 (and line 9 using the shortcut). Here are the (partial) screen output of the Python script

```
Indian cyclic method (last 3 lines)
line: 21 r: 12 s:  35 K:  5 P:18871580499429    Q:1807569584602
line: 22 r:  8 s: -45 K: -9 P:69599545743410    Q:6666427435249
line: 23 r: 10 s:  -9 K:  1 P:158070671986249   Q:15140424455100

Indian cyclic method (last 3 lines) with shortcut
line:  6 r: 11 s:  12 K: -3 P:1399              Q:134
line:  7 r: 10 s:  -9 K:  3 P:9532              Q:913
Final line: K:  1 P:158070671986249 Q:15140424455100

English method (last 3 lines)
line: 29 r:  7 s: -60 K:  5 P:18871580499429    Q:1807569584602
line: 30 r:  8 s: -45 K: -9 P:69599545743410    Q:6666427435249
line: 31 r: 10 s:  -9 K:  1 P:158070671986249   Q:15140424455100

English method (last 3 lines) with shortcut
line:  8 r:  8 s: -45 K: -3 P:1399              Q:134
line:  9 r: 10 s:  -9 K:  3 P:9532              Q:913
Final line: K:  1 P:158070671986249 Q:15140424455100
```

Page 38, Problem 1. Show that the only integral solutions to $1 + x + x^2 + x^3$ being a square is $x = -1, 0, 1, 7$. First, some factorization

$$\begin{aligned}
1 + x + x^2 + x^3 &= (1 + x + x^2) + x^3 \\
&= (1 + x)^2 - x + x^3 = (1 + x)^2 - x(1 - x^2) \\
&= (1 + x)^2 - x(1 + x)(1 - x) \\
&= (1 + x)[(1 + x) - x(1 - x)] = (1 + x)[1 + x - x + x^2] \\
&= (1 + x)(1 + x^2)
\end{aligned}$$

From here we can conclude that x cannot be even unless $x = 0$, here's how, we know that $A^2 = (1 + x)(1 + x^2)$ and suppose that d is the common factor of $(1 + x)$ and $(1 + x^2)$, therefore d also divides

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

thus $d|2$ or $d|x$. But here x is even, thus $1+x$ is odd, do d can't divide 2, so $d|x$ but since $d|(1+x)$ and x and $1+x$ are co-prime, $d=1$. This means that

$$1+x=y^2$$
$$1+x^2=z^2$$

the last equation means $z^2-x^2=1$ but the difference between two squares cannot be one unless $x=0$. Thus is x is even then $x=0$.

Next is x odd. Let's recast $x=2m+1$, we then have

$$\begin{aligned} A^2=1+x+x^3+x^3=(1+x)(1+x^2)&=(1+2m+1)(1+(2m+1)^2)\\ &=2(m+1)(4m^2+4m+2)\\ &=4(m+1)(2m^2+2m+1)\\ \rightarrow A^2&=4(m+1)(m^2+(m+1)^2) \end{aligned}$$

Let's divide out the factor of 4 and we have

$$A'^2=(m+1)(m^2+(m+1)^2)$$

any factor of $m+1$ and $m^2+(m+1)^2$ would also divide m^2 but $m+1$ and m^2 are co-prime thus $(m+1)$ and $m^2+(m+1)^2$ are co-prime thus each of them is square

$$m+1=w^2$$
$$m^2+(m+1)^2=y^2$$

since m and $m+1$ are co-prime, $m^2+(m+1)^2=y^2$ forms a primitive Pythagorean triple, therefore we can cast it in the usual form, but here we have two choices, either m is even or m is odd. First, let's tackle the m even

$$m=2ab$$
$$m+1=a^2-b^2=w^2$$

since from above we know that $m+1$ is square and

$$\begin{aligned} (m+1)-m=1&=a^2-b^2-2ab\\ 1&=(a-b)^2-2b^2 \end{aligned}$$

This is a form of Pell's equation and I was messing around with Pell's equation for roughly two days until I found out that I don't need to mess with Pell's equation at all. We'll talk about Pell's equation later :)

What we need here is to note that since $m+1 = w^2 = a^2 - b^2$, so it forms another Pythagorean triple, since a and b are co-prime, they are also primitive

$$a = c^2 + d^2$$
$$b = 2cd$$

therefore the Pell's equation we had earlier becomes

$$\begin{aligned} 1 &= (a-b)^2 - 2b^2 \\ &= (c^2 + d^2 - 2cd)^2 - 2(2cd)^2 \\ &= (c-d)^4 - 8(cd)^2 \end{aligned}$$

we now do the oldest trick in the book, substitutions

$$s = c + d \qquad\qquad t = c - d$$

therefore $st = c^2 - d^2$ and

$$s + t = 2c \qquad\qquad s - t = 2d$$

and

$$\begin{aligned} (s+t)(s-t) = s^2 - t^2 &= 4cd \\ \rightarrow \frac{s^2 - t^2}{4} &= cd \end{aligned}$$

making the substitution

$$\begin{aligned} 1 = (c-d)^4 - 8(cd)^2 = t^4 - 8\left(\frac{s^2 - t^2}{4}\right)^2 \\ 1 = t^4 - \frac{1}{2}\left(s^2 - t^2\right)^2 \\ \rightarrow 2 = 2t^4 - \left(s^2 - t^2\right)^2 \end{aligned}$$

at this point I was quite stuck until I tried the simplest solution, the quadratic formula, solving for s we get

$$s = \pm\sqrt{t^2 \pm \sqrt{2}\sqrt{t^4 - 1}}$$

for s to have a chance to be an integer we need $\sqrt{2}\sqrt{t^4-1}$ to be an integer, therefore

$$t^4 - 1 = 2Q^2$$
$$(t^2-1)(t^2+1) = 2Q^2$$

but $t = c - d$ and c and d are of opposite parities, thus t is odd and $\gcd(t^2-1, t^2+1) = 2$ thus one of t^2-1 and t^2+1 is a square and the other is 2 times a square but either way we cannot have $t^2 \pm 1$ equal a square unless $t = 0$ or $t = \pm 1$. But from the original Pell's equation $2 = 2t^4 - (s^2 - t^2)$ if $t = 0$ we have no solution for s. If $t = \pm 1$ then $s = \pm 1$ as well (or ∓ 1).

But from $s = c + d$ it has to be positive (remember that c and d are part of a Pythagorean triple), thus $s = 1$, so one of c or d must be zero. From $b = 2cd$ we have $b = 0$ and the original Pell's equation gets to

$$\begin{aligned} 1 &= (a-b)^2 - 2b^2 \\ &= (a-0)^2 - 2 \cdot 0^2 \\ \rightarrow 1 &= a \end{aligned}$$

and from $m + 1 = w^2 = a^2 - b^2$ we have $m + 1 = 1$ and $m = 0$ and from $x = 2m + 1$ we have $x = 1$. Thus we so far had $x = 0$ and $x = 1$ as solutions.

Next, we tackle $x = 2m + 1$ odd with m odd, thus like the previous case

$$m = a^2 - b^2$$
$$m + 1 = 2ab = w^2$$

and they obey a (negative) Pell's equation just like above

$$\begin{aligned} m + 1 - m = 1 &= 2ab - (a^2 - b^2) \\ &= 2b^2 - (a-b)^2 \end{aligned}$$

since a and b are co-prime we have either $a = 2A^2$ and $b = B^2$ or $a = A^2$ and $b = 2B^2$ but if it is the latter then from the Pell's equations

$$\begin{aligned} 1 &= 2b^2 - (a-b)^2 \\ &= (2B)^2 - (A^2 - 2B^2)^2 \end{aligned}$$

but again, the difference of two squares cannot be one unless $2B = 1$ and $A^2 - 2B^2 = 0$ but this is impossible since A and B are integers, therefore $b = B^2$ and $a = 2A^2$ and we have

$$1 = 2B^4 - (A^2 - 2B^2)^2$$

again I was messing with Pell's equations again but again it was not needed, quadratic formula to the rescue! solving for B we get

$$B = \pm\sqrt{-2A^2 \pm \sqrt{8A^4 + 1}}$$

for B to be an integer we must have $8A^4 + 1$ to be a square, on the outset it is nothing more than just a Pell's equation but we can do better, borrowing the trick I used in solving $y^2 = x^3 + 1$, we do the following

$$\begin{aligned} 8A^4 + 1 &= k^2 \\ 8A^4 &= k^2 - 1 \\ &= (k-1)(k+1) \\ \rightarrow 8A^4 &= n(n+2) \end{aligned}$$

where $n = k - 1$. We know that $\gcd(n, n+2)$ is at most 2 but since the LHS is $8A^4$ it must be 2 :) So we need to distribute the prime factors of $8A^4$ into n and $n+2$ and since $\gcd(n, n+2) = 2$ we must have either

$$n = 2C^4 \qquad n + 2 = 2^{4r+2}D^4 \qquad \text{or} \qquad n = 2^{4r+2}D^4 \qquad n + 2 = 2C^4$$

the 2^{4r+2} is to make sure that when we multiply n and $n + 2$ we get an overall factor 8, also from their difference $n + 2 - n = 2$ we get (including the two cases)

$$\begin{aligned} \pm 2 &= 2C^4 - 2^{4r+2}D^4 \\ \rightarrow \pm 1 &= C^4 - 2E^4, \qquad E^4 = 2^{4r}D^4 \end{aligned}$$

at this point we will generalize things, since we can think of $1 = 1^4$, I wanted to see if there are solutions to the following equations

$$2E^4 = C^4 + F^4 \qquad \text{and} \qquad 2E^4 = C^4 - F^4$$

Now, if C and F are both even, then we can cancel an overall factor of 2^4 throughout (the same with any common factor between them), and if after canceling they still contain 2 we can do the same until we reach a point where C and F are both odd and co-prime. They must be both odd because the LHS is even.

So we can just consider co-prime solutions with C and F odd. Since they are both odd

$$\begin{aligned} C + F &= 2u & C - F &= 2v \\ C &= u + v & F &= u - v \end{aligned}$$

with u, v of opposite parities and co-prime since their sum (and difference) is odd and C and F are co-prime. Now tackling the first case $2E^4 = F^4 + C^4$ we get

$$\begin{aligned} 2E^4 &= (u+v)^4 + (u-v)^4 \\ \cancel{2}E^4 &= \cancel{2}(u^4 + 6u^2v^2 + v^4) \\ E^4 &= (u^2+v^2)^2 + (2uv)^2 \end{aligned}$$

but since u and v are co-prime and of opposite parities they form a Pythagorean triple

$$\begin{aligned} (u^2-v^2)^2 + (2uv)^2 &= (u^2+v^2)^2 \\ (u^2-v^2)^2 &= (u^2+v^2)^2 - (2uv)^2 \end{aligned}$$

multiplying both of them

$$\begin{aligned} (E^2)^2(u^2-v^2)^2 &= \left[(u^2+v^2)^2 + (2uv)^2\right]\left[(u^2+v^2)^2 - (2uv)^2\right] \\ \left[(E^2)(u^2-v^2)\right]^2 &= (u^2+v^2)^4 - (2uv)^4 \end{aligned}$$

but we know that $Z^2 = Y^4 - X^4$ has no non-trivial solutions, the only trivial solutions are all zeroes (which we cannot have here since $Y = u^2 + v^2$), the other trivial solution $Z = 1$ and $Y = 1$ with $X = 0$.

This means that $2uv = 0$ so either $u = 0$ or $v = 0$ or both (but we can't have both zero because we need $Y = u^2 + v^2$ to be 1). But from $C = u + v$ and $F = u - v$, if one of them is zero we have $C = \pm F = \pm 1$, either way, from $2E^4 = C^4 + F^4$ we have $E = 1$.

And from $n = 2C^4 = 2, n + 2 = 4E^4 = 4$ (or the other way round) we get $8A^4 = n(n+2) = 8$, meaning $A = 1$. And from $B = \pm\sqrt{-2A^2 \pm \sqrt{8A^4 + 1}}$, we get $B = \pm 1$

which in turn means $m = a^2 - b^2 = 4A^4 - B^2 = 3$ and $m + 1 = 2ab = 4A^2B^2 = 4$, this translates to $x = 2m + 1 = 7$.

The other case is $2E^4 = C^4 - F^4$, again substituting $C = u + v$ and $F = u - v$

$$\begin{aligned} 2E^4 &= (u+v)^4 - (u-v)^4 \\ &= 8uv(u^2+v^2) \\ \rightarrow E^4 &= 4uv(u^2+v^2) \end{aligned}$$

now u is co-prime to $u^2 + v^2$ and v is also co-prime to $u^2 + v^2$ also $u^2 + v^2$ is odd so it is also co-prime to 4, therefore $4uv$ is co-prime to $u^2 + v^2$, thus

$$\begin{aligned} 4uv &= H^4 \\ u^2 + v^2 &= I^4 \end{aligned}$$

but u and v are co-prime and of opposite parities, say v is odd, from $4uv = H^4$ we must have $v = V^4$ and from the second equation we therefore have $u^2 + (V^2)^4 = I^4$ but again $Z^2 = Y^4 - X^4$ has only trivial solutions. Again the all zero solution is out because then $u = v = 0$ but they must be of opposite parities.

The other trivial solution is $Y = I = 1 \rightarrow v = 1$ and $Z = v = 0$ and $X = u = 1$, this means $C = u + v = 1$ and $F = u - v = 1$ and $2E^4 = C^4 - F^4 = 1 - 1 = 0 \rightarrow E = 0$, which means one of n or $n+2$ is zero, which also means $8A^4 = n(n+2) = 0 \rightarrow A = 0$ and $B = \pm\sqrt{-2A^2 \pm \sqrt{8A^4 + 1}} = \pm 1$. This means that $m = a^2 - b^2 = 4A^4 - B^2 = -1$ and $m + 1 = 2ab = 4A^2B^2 = 0$ and $x = 2m + 1 = -1$ and this is FINALLY our last solution LOL.

In short, from this exercise the valid values of m are $-1, 0, 3$, this will be useful in the future :)

Pell's Equation Permutation. Obviously we encountered Pell's equations along the way of the form $x^2 - 2y^2 = \pm 1$ in this problem. So I learned a thing or two about solving Pell's equation, well not really in solving it because for that you'll need the Indian cyclic method or the English method but here is how we generate more solutions once we get the first one, note that

$$1 = x^2 - ny^2 = (x + \sqrt{n}y)(x - \sqrt{n}y)$$

so say we get a first solution x_0, y_0 we can exponentiate it to get the k^{th} one, $(x_0+\sqrt{n}y_0)^k = x_k + \sqrt{n}y_k$ (we can also choose to do it with a negative sign $(x_0 - \sqrt{n}y_0)^k = x_k - \sqrt{n}y_k$), this is why, from Pell's equation we know that

$$\begin{aligned} 1 &= (x_0 + \sqrt{n}y_0)(x_0 - \sqrt{n}y_0) \\ \rightarrow 1^k &= (x_0 + \sqrt{n}y_0)^k(x_0 - \sqrt{n}y_0)^k \end{aligned}$$

the two brackets on the RHS will yield the same x_k, y_k because

$$\begin{aligned} (x_0 \pm \sqrt{n}y_0)^k &= \sum_{i=0}^{k} (\pm 1)^i \binom{k}{i} x_0^{k-i} y_0^i n^{\frac{i}{2}} \\ &= \sum_{i=0}^{\lfloor k/2 \rfloor} (\pm 1)^{2i} \binom{k}{2i} x_0^{k-2i} y_0^{2i} n^{\frac{2i}{2}} + \sum_{i=0}^{\lfloor (k-1)/2 \rfloor} (\pm 1)^{2i+1} \binom{k}{2i+1} x_0^{k-2i-1} y_0^{2i+1} n^{\frac{2i+1}{2}} \\ &= \left\{ \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{2i} x_0^{k-2i} y_0^{2i} n^i \right\} \pm \sqrt{n} \left\{ \sum_{i=0}^{\lfloor (k-1)/2 \rfloor} \binom{k}{2i+1} x_0^{k-2i-1} y_0^{2i+1} n^i \right\} \\ &= x_k \pm \sqrt{n} y_k \end{aligned}$$

we are just basically splitting the sum to even and odd indices, and we saw above that $(x_0+\sqrt{n}y_0)^k$ and $(x_0-\sqrt{n}y_0)^k$ generate the same x_k, y_k such that when we multiply them

$$\begin{aligned} 1^k &= (x_0 + \sqrt{n}y_0)^k(x_0 - \sqrt{n}y_0)^k \\ 1 &= (x_k + \sqrt{n}y_k)(x_k - \sqrt{n}y_k) \\ &= x_k^2 - ny_k^2 \end{aligned}$$

For $n = 2$ we can use the above formula but more than that we can actually derive a recurrence relation $x_{n+2} = 6x_{n+1} - x_n$, the same applies to $y_{n+2} = 6y_{n+1} - y_n$. Although we also had the negative Pell's equation as well $x^2 - 2y^2 = \pm 1$, the first 9 solutions can be found on Table. III. How do we prove this recurrence relation, say with induction?

$$\begin{aligned} x_{n+2}^2 - 2y_{n+2}^2 &= (6x_{n+1} - x_n)^2 - 2(6y_{n+1} - y_n)^2 \\ &= (6^2 x_{n+1}^2 + x_n^2 - 2x_{n+1}x_n) - 2(6^2 y_{n+1}^2 + y_n^2 - 2y_{n+1}y_n) \end{aligned}$$

The somewhat problematic terms here are the crossed ones

$$\begin{aligned} x_{n+1}x_n &= (6x_n - x_{n-1})x_n \\ &= 6x_n^2 - x_{n-1}x_n \\ &= 6x_n^2 - x_{n-1}(6x_{n-1} - x_{n-2}) \\ &= 6x_n^2 - 6x_{n-1}^2 + \cdots + (-1)^n x_1 x_0 \end{aligned}$$

The same of course goes with y_{n+2}, going back to $x_{n+2}^2 - 2y_{n+2}^2$ we get

$$\begin{aligned} x_{n+2}^2 - 2y_{n+2}^2 &= (6^2 x_{n+1}^2 + x_n^2 - 2 \cdot 6 x_{n+1}x_n) - 2(6^2 y_{n+1}^2 + y_n^2 - 2 \cdot 6 y_{n+1}y_n) \\ &= 6^2(x_{n+1}^2 - 2y_{n+1}^2) + (x_n^2 - 2y_n^2) - 12(-1)^n(x_1x_0 - 2y_1y_0) - 12\sum_{i=1}^{n}(-1)^{i+n}6(x^2 - 2y^2) \\ &= \pm 6^2 \pm 1 - 12(-1)^n(x_1x_0 - 2y_1y_0) - 12\sum_{i=1}^{n}(-1)^{i+n}(\pm 6) \end{aligned}$$

the $\pm 6^2$, ± 1 in the middle and the ± 6 in the sum depend on $x^2 - 2y^2 = \pm 1$, the last sum is either 0 or ± 6 depending on whether n is even or odd respectively. So if n is even we have

$$x_{n+2}^2 - 2y_{n+2}^2 = \begin{cases} 6^2 + 1 - 12(1 \cdot 3 - 20 \cdot 2) = 1 & \text{for } x^2 - 2y^2 = 1 \\ -6^2 - 1 - 12(1 \cdot 7 - 2 \cdot 1 \cdot 5) = -1 & \text{for } x^2 - 2y^2 = -1 \end{cases}$$

if n is odd we have

$$x_{n+2}^2 - 2y_{n+2}^2 = \begin{cases} 6^2 + 1 + 12(1 \cdot 3 - 20 \cdot 2) - 12 \cdot 6 = 1 & \text{for } x^2 - 2y^2 = 1 \\ -6^2 - 1 + 12(1 \cdot 7 - 2 \cdot 1 \cdot 5) + 12 \cdot 6 = -1 & \text{for } x^2 - 2y^2 = -1 \end{cases}$$

and the induction is complete (note that we get the values for x_0, x_1, y_0, y_1 from Table. III above).

I initially wanted to show that the solutions to $x^2 - 2y^2 = \pm 1$ are actually not bi-quadratic, *i.e.* I wanted to show that x (or maybe y can't remember which one) cannot be a square. I tried using any odd methods, like listing all the values and then modding them mod 10, 4, 6, 16, etc because for a number to be square it must be $0, 1, 4, 9$ mode 16, $1, 3$ mod 6, etc, but there's always a number that satisfy all of them mods LOL. I also tried showing that $x^2 - 2(y^2)^2 = -1$ has no solution but I was wrong since from

TABLE III: Solutions to left $x^2 - 2y^2 = 1$ and right $x^2 - 2y^2 = -1$

x	y	x	y
1	0	1	1
3	2	7	5
17	12	41	29
99	70	239	169
577	408	1393	985
3363	2378	8119	5741
19601	13860	47321	33461
114243	80782	275807	195025
665857	470832	1607521	1136689

Table. III we see that we have $y^2 = 169$, the thing is that we had more constraints, *i.e.* $x = 2A^2 - B^2$ and this is the one not satisfied by this particular solution.

Another thing I noticed was that the rightmost y in Table. III is also the hypotenuse of a right triangle whose legs differ by one. Note that we initially had $m^2 + (m+1)^2 = Y^2$ and $m = 2ab$, $m+1 = a^2 - b^2$ or the other way round, and it generates the Pell's equations $(a-b)^2 - 2b^2 = \pm 1$. But the funny thing is that the hypotenuse itself, as a result of these Pell's equation, has the values of the solutions of the Pell's equations themselves, it looked mysterious but it is actually not, because the hypotenuse itself also obeys the same Pell's equation, because

$$\begin{aligned} x^2 + (x+1)^2 &= y^2 \\ 2x^2 + 2x + 1 &= y^2 \\ (2x+1)^2 - 2x^2 - 2x &= y^2 \\ (2x+1)^2 - 2x^2 - 2x - 1 + 1 &= y^2 \\ (2x+1)^2 - y^2 + 1 &= y^2 \\ \rightarrow (2x+1)^2 - 2y^2 &= -1 \end{aligned}$$

so the lesson is if some variable has the same values as a solution to a certain equation,

then it *must* also be a solution :)

Another thing I tried was to reapply Pell's equation to $\sqrt{8A^4+1} = \sqrt{2(2A^2)^2+1}$ above. And it got nowhere fast, the results I got was that this also means that half of the solution to y in $x^2 - 2y^2 = 1$ must also be a square, *i.e.* $\frac{1}{2}y = h^2$. But again it got nowhere even faster. But on the flip side the result above (as long as I don't miss any assumptions in applying it to this case) shows that $\frac{1}{2}y$ with y on the left of Table. III cannot be square :)

I tried other approaches as well. My very first attempt was actually to use geometric series $1 + x + x^2 + x^3 = (x^4 - 1)/(x - 1)$ but then I wasn't sure what to do next. And others are not even worth mentioning :)

Basic and Extra Ingredients

The knowledge needed to solve this problem (my way) is

- Factorization, $1 + x + x^2 + x^3 = (1 + x)(1 + x^2)$
- Even odd classifications, what happens if x is odd, what happens if x is even
- Pythagorean triples, $m^2 - n^2, 2mn, m^2 + n^2$
- Quadratic formula, $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$
- $Z^2 = Y^4 - X^4$ has only trivial solutions
- Prime factorization implication, $8A^4 = n(n + 2) \rightarrow n = 2C^4, n + 2 = 2^{4n+2}D^4$
- Generalization, $2E^4 = C^4 - 1 \rightarrow 2E^4 = C^4 - F^4$ and find that the latter has no solution

Note that I already knew all these, the trick is what to use and when :) and of course Pell's equation is not even needed

Sinister problems :)

Sometimes I wonder, without knowing the above solution, what happens if the following problems are presented, would someone be able to solve them?

1. Prove that the following hypotenuses are all the hypotenuses of right triangles whose legs differ by one, 1, 5, 29, 169, 985, 5741, 33461, 195025, 1136689, etc or in other words they obey the following recurrence relation $h_{n+2} = 6h_{n+1} - h_n$

2. Prove that each number in the following sequence, 0, 1, 6, 35, 204, 1189, 6930, 40391, 235416, etc, is not a square, except for 0 and 1.

I guess the lesson is that it's harder to prove that a sequence of numbers is not squares than to prove that certain equation $2E^4 = C^4 + F^4$ has no non-trivial integer solutions.

Since $t = c - d$

Chapter 4

This is one of the main chapters.

Page 76. Factorization of $x^n + y^n$ using roots of unity. This only works for odd n because we start with

$$X^n - 1 = (X - 1)(X - r)\dots(X - r^{n-1})$$

we then set $X = -\frac{x}{y}$

$$\left(-\frac{x}{y}\right)^n - 1 = (-\frac{x}{y} - 1)(-\frac{x}{y} - r)\dots(-\frac{x}{y} - r^{n-1})$$
$$\rightarrow (-1)^n\frac{x^n}{y^n} - 1 = (-1)^n(\frac{x}{y} + 1)(\frac{x}{y} + r)\dots(\frac{x}{y} + r^{n-1})$$

and multiply by $-y^n$, if n is odd then we get

$$x^n + y^n = (x + y)(x + ry)\dots(x + r^{n-1}y)$$

but if n is even we get

$$x^n - y^n = (x + y)(x + ry)\dots(x + r^{n-1}y)$$

the real culprit is the fact that we start with a minus sign $X^n - 1$. For n even we have to start with the roots of -1 rather than the roots of $+1$, so

$$X^n + 1 = (X + s)(X + sr)\dots(X + sr^{n-1})$$

where $s = e^{\pi i/n}$ and r is like before the roots of 1 (whart we're doing is basically rotating the roots of 1 90° counter clockwise), $e^{2\pi i/n}$ we can then proceed like before, setting $X = \frac{x}{y}$ and then multiplying by y^n.

Page 86, Problem 1. This is straightforward enough. Here we have $\lambda = 5$ and $2+\alpha+3\alpha^2-2\alpha^3 = -\alpha+\alpha^2-4\alpha^3-2\alpha^4$. What we want here is to show that $f(\alpha^3) = g(\alpha^3)$ where $f(\alpha)$ is the LHS and $g(\alpha)$ is the RHS.

Comparing the coefficients of both sides we see that the LHS is the second form, *i.e.* we remove the highest power of α and the constant offset $c = -2$.

Plugging in α^3 in place of α we get

$$2 + \alpha^3 + 3\alpha^6 - 2\alpha^9 = -\alpha^3 + \alpha^6 - 4\alpha^9 - 2\alpha^{12}$$
$$2 + \alpha^3 + 3\alpha - 2\alpha^4 = -\alpha^3 + \alpha - 4\alpha^4 - 2\alpha^2$$

massaging the RHS we get (knowing that $c(1 + \alpha + \cdots + \alpha^{\lambda-1}) = 0$ and choosing $c = 2$)

$$-\alpha^3 + \alpha - 4\alpha^4 - 2\alpha^2 + 2(1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4) = 2 + \alpha^3 + 3\alpha - 2\alpha^4$$

which is the LHS.

The next part of the problem asks if $f(\alpha^5) = g(\alpha^5)$, the answer is obviously not because $\alpha^5 = 1$ and so any term with α in it becomes that term multiplied by one

$$2 + 1 + 3 - 2 \neq -1 + 1 - 4 - 2$$

Page 86, Problem 2. This is a good thing to be implemented in Python, something that I will need for Problem 5, so I'll put the actual script on problem 5 itself. Here I'll just use the script to calculate the multiplications. First, denote the cyclotomic integers as

$$A = \alpha^4 + 7\alpha^2 + 5\alpha + 1$$
$$B = 2\alpha^3 + 3\alpha^2 - \alpha + 2$$
$$C = 4\alpha^4 + 2\alpha^3 - \alpha^2 + 5$$

First we will calculate $(AB)C$ and then $A(BC)$

$$AB = 33\alpha^4 + 10\alpha^3 + 14\alpha^2 + 12\alpha + 15$$
$$BC = 3\alpha^4 + 15\alpha^3 + 21\alpha^2 + 11\alpha + 10$$
$$\rightarrow (AB)C = A(BC) = 235\alpha^4 + 200\alpha^3 + 161\alpha^2 + 103\alpha + 141$$

Page 87, Problem 3. Here we want to show that for $\lambda = 3$ the norm is always of the form $\frac{1}{4}(A^2 + 3B^2)$ and that A and B have the same parity (both odd or both even).

The same parity part is easy because there's a $\frac{1}{4}$ multiplying the whole thing, if A and B differ in parity, then $(A^2 + 3B^2) \not\equiv 0 \mod 4$.

It took me some time to figure this one out. Here's why. I started out naively

$$\begin{aligned} Nf(\alpha) = f(\alpha)f(\alpha^2) &= (b_0 + b_1\alpha + b_2\alpha^2)(b_0 + b_1\alpha^2 + b_2\alpha) \\ &= b_0^2 + b_1^2 + b_2^2 + \alpha(b_0b_1 + b_0b_2 + b_1b_2) + \alpha^2(b_0b_1 + b_0b_2 + b_1b_2) \\ &= b_0^2 + b_1^2 + b_2^2 + (\alpha + \alpha^2)(b_0b_1 + b_0b_2 + b_1b_2) \\ &= b_0^2 + b_1^2 + b_2^2 + (-1)(b_0b_1 + b_0b_2 + b_1b_2) \end{aligned}$$

since $1 + \alpha + \alpha^2 = 0$. Moving on

$$b_0^2 + b_1^2 + b_2^2 - (b_0b_1 + b_0b_2 + b_1b_2) = (b_0 + b_1 + b_2)^2 - 3(b_0b_1 + b_0b_2 + b_1b_2)$$

This made me happy for a while since one term is a square and the other has a three in front of it. However, the term multiplying the 3 can be negative depending on what the b's are and in our case we want it to be a square as well.

I then remembered that only primes of the form $6n + 1$ can be expressed as $x^2 + 3y^2$. So if I can show that $Nf(\alpha)$ is only divisible by 3, 4 and primes of the form $6n + 1$ I'm good to go. But this is not easy to show.

I then went brute force, doing everything mod 6 we have a total of 216 combinations of b_0, b_1, b_2 to check, a bit much. But we can express $f(\alpha)$ ins the second form where we do away with the α^2 term, in this case we have $f(\alpha) = c_0 + c_1\alpha$ and $Nf(\alpha) = c_0^2 + c_1^2 - c_0c_1$ so we only have 6 choose 2 = 15 combinations to check, choose 2 because it is symmetric in $c_0 \leftrightarrow c_1$.

I actually computed all 15 combinations, the results are $0, 1, 3, 4 \mod 6$. The $0, 4 \mod 6$ cases happen only when $c_{0,1}$ are even so we can redo them using $2, 0 \mod 4$.

However, what we need is to show that every prime factor of $Nf(\alpha)$ is $1 \mod 6$, something which was too hard.

The answer came after I realized that we might be able to do our usual trick in separating c_0c_1,

$$c_1 + c_0 = u$$
$$c_1 - c_0 = v$$

which gives us $c_1 = \frac{u+v}{2}$ and $c_0 = \frac{u-v}{2}$, substituting this into $Nf(\alpha) = c_0^2 + c_1^2 - c_0c_1$ we get

$$\begin{aligned} Nf(\alpha) &= \frac{1}{4}(u^2 - 2uv + v^2 + u^2 + 2uv + v^2 - u^2 + v^2) \\ &= \frac{1}{4}(u^2 + 3v^2) \end{aligned}$$

and that's our answer.

Next is to find all six units for $\lambda = 3$. The units are given by $Nf(\alpha) = \frac{1}{4}(u^2+3v^2) = 1$, so the only possible values are

$$\begin{array}{llllll} u = 1 & v = 1 & \to & c_1 = 1 & c_0 = 0 \\ u = 1 & v = -1 & \to & c_1 = 0 & c_0 = 1 \\ u = -1 & v = 1 & \to & c_1 = 0 & c_0 = -1 \\ u = -1 & v = -1 & \to & c_1 = -1 & c_0 = 0 \\ u = 2 & v = 0 & \to & c_1 = 1 & c_0 = 1 \\ u = -2 & v = 0 & \to & c_1 = -1 & c_0 = -1 \end{array}$$

where $f(\alpha) = c_0 + c_1\alpha$.

Page 87, Problem 4. We now need to do what we did for Problem 3 but for $\lambda = 5$ and the final goal is to show that $Nf(\alpha) = \frac{1}{4}(A^2 - 5B^2)$. Also we have the hint this time so I'll just follow the hint. The only extra thing I'd do is cast $f(\alpha)$ in the second form where we remove the α^4 term, $f(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3$.

Multiplying $f(\alpha)f(\alpha^4)$ we get

$$b_0^2 + b_1^2 + b_2^2 + b_3^2 + (\alpha + \alpha^4)(b_0b_1 + b_1b_2 + b_2b_3) + (\alpha^2 + \alpha^3)(b_0b_3 + b_0b_2 + b_1b_3)$$

Note that $\theta_0 = \alpha + \alpha^4$ is real because they are complex conjugate of one another, the same goes with $\theta_1 = \alpha^2 + \alpha^3$. Thus $a = b_0^2 + b_1^2 + b_2^2 + b_3^2$, $b = b_0b_1 + b_1b_2 + b_2b_3$ and $c = b_0b_3 + b_0b_2 + b_1b_3$.

Doing $f(\alpha^2)f(\alpha^3)$ will give us $a + b\theta_1 + c\theta_0$ indeed. The confusing thing about the hint is that the norm will be of the form $(b\theta_0 + c\theta_1)(b\theta_1 + c\theta_0)$. I finally realized that the b and c here are not the b and c above, that's why he used the phrase "the norm has the form" rather than "the norm is".

One thing to note is that

$$\theta_0 + \theta_1 = \alpha + \alpha^4 + \alpha^2 + \alpha^3 = -1$$

because $1 + \alpha + \cdots + \alpha^4 = 1$. Therefore, we can rewrite $f(\alpha)f(\alpha^4)$ as

$$\begin{aligned} a + b\theta_0 + c\theta_1 &= -a(\theta_0 + \theta_1) + b\theta_0 + c\theta_1 \\ &= (b-a)\theta_0 + (c-a)\theta_1 \end{aligned}$$

the same with $f(\alpha^2)f(\alpha^3) = (b-a)\theta_1 + (c-a)\theta_0$, let $m = b - a$ and $n = c - a$ thus

$$\begin{aligned} Nf(\alpha) = f(\alpha)f(\alpha^4) \cdot f(\alpha^2)f(\alpha^3) &= (m\theta_0 + n\theta_1)(m\theta_1 + n\theta_0) \\ &= m^2\theta_1\theta_0 + mn(\theta_0^2 + \theta_1^2) + n^2\theta_1\theta_0 \end{aligned}$$

Now

$$\begin{aligned} \theta_0\theta_1 &= (\alpha + \alpha^4)(\alpha^2 + \alpha^3) \\ &= \alpha^3 + \alpha^4 + \alpha + \alpha^2 \\ &= -1 \end{aligned}$$

and

$$\begin{aligned} \theta_0^2 &= (\alpha + \alpha^4)^2 = \alpha^2 + 2\alpha^5 + \alpha^3 \\ \theta_1^2 &= (\alpha^2 + \alpha^3)^2 = \alpha^4 + 2\alpha^5 + \alpha \\ \rightarrow \theta_0^2 + \theta_1^2 &= \alpha^2 + \alpha^3 + \alpha + \alpha^4 + 4 = -1 + 4 \\ &= 3 \end{aligned}$$

Thus

$$m^2\theta_1\theta_0 + mn(\theta_0^2 + \theta_1^2) + n^2\theta_1\theta_0 = -m^2 + 3mn - n^2$$

again, using the usual trick $m+n=u$ and $m-n=v \rightarrow m=\frac{u+v}{2}$ and $n=\frac{u-v}{2}$ we get

$$\begin{aligned} -m^2+3mn-n^2 &= \frac{1}{4}(-u^2-2uv-v^2-u^2+2uv-v^2+3u^2-3v^2) \\ &= \frac{1}{4}(u^2-5v^2) \end{aligned}$$

which is what we want. We now need to find the units which in this case satisfy $\frac{1}{4}(u^2-5v^2)=1$ or $u^2-5v^2=4$. The good news is that we can use Pell's equation $r^2-5s^2=1$ and then multiply everything by four $(2r)^2-5(2s)^2=2^2$ in this way we get infinite number of units from the infinite number of solutions to Pell's equation. The drawback here is that the solutions are all even $u=2r$ and $v=2s$.

Page 87, Problem 5. Here $\lambda=7$ and $f(\alpha)=\alpha^5-\alpha^4-3\alpha^2-3\alpha-2$, and here we need to compute $Nf(\alpha)$. Here we have a slightly different hint than that of Problem 4. We group $Nf(\alpha)$ by $f(\alpha)f(\alpha^2)f(\alpha^4)$ rather than by their complex conjugates like in Problem 4 $f(\alpha)f(\alpha^6)$.

But looks like there a bug in this book, I've calculated the norm of $f(\alpha)$ multiple times and it is not 2509 instead it is 1247. Anyway, first thing I did was write a Python program to do this as follows

```
# shifts f(A) to f(A^k), k > 0
def cycShift(f, k):

    if (k <= 0) or len(f) <= 0:
        return
    if (k == 1):
        return f

    L = len(f)
    g = [0] * L

    for i in xrange(L):
        g[(i*k) % L] += f[i]

    return g


# multiplies two f's
def multCyc(f, g):

    if len(f) != len(g):
        return

    L = len(f)
    res = [0] * L

    for i in xrange(L):
```

```
        for j in xrange(L):
            res[(i+j) %L] += (g[i] * f[j])

    return res

# add two f's
def addCyc(f, g):

    if len(f) != len(g):
        return

    L = len(f)
    res = [0] * L

    for i in xrange(L):
        res[i] = g[i] + f[i]

    return res

# compute norm of f(A)
def cycNorm(f):

    L = len(f)

    if L <= 1:
        return

    res = [i for i in f] # deep copy of f

    # create f(A^k)
    for k in xrange(2,L):
        fk = cycShift(f, k)
        res = multCyc(res, fk)

    for k in xrange(3,L):
        if res[k] != res[k-1]:
            return

    return res[0] - res[1]
```

If we do what the book suggested we get

$$f(\alpha)f(\alpha^2)f(\alpha^4) = -87(\alpha^6 + \alpha^5 + \alpha^3) - 65(\alpha^4 + \alpha^2 + \alpha) - 56$$
$$f(\alpha^3)f(\alpha^5)f(\alpha^6) = -87(\alpha^4 + \alpha^2 + \alpha) - 65(\alpha^6 + \alpha^5 + \alpha^3) - 56$$

Thus we can choose $\theta_0 = \alpha^6 + \alpha^5 + \alpha^3$ and $\theta_1 = \alpha^4 + \alpha^2 + \alpha$, just like Problem 4 we have $\theta_0 + \theta_1 = -1$ so we can express

$$-56 = 56(\theta_0 + \theta_1)$$

and so

$$f(\alpha)f(\alpha^2)f(\alpha^4)\cdot f(\alpha^3)f(\alpha^5)f(\alpha^6) = (-31\theta_1 - 9\theta_0)(-31\theta_0 - 9\theta_1)$$
$$= 31^2\theta_0\theta_1 + 31\cdot 9(\theta_0^2+\theta_1^2) + 9^2\theta_1\theta_0$$

using the identities

$$\theta_0\theta_1 = \alpha^3+\alpha+1+\alpha^2+1+\alpha^6+1+\alpha^5+\alpha^4 = 2$$
$$\theta_0^2 = \alpha^5+\alpha^3+\alpha^6+2(\alpha^4+\alpha^2+\alpha)$$
$$\theta_1^2 = \alpha+\alpha^4+\alpha^2+2(\alpha^6+\alpha^5+\alpha^3)$$

and so $\theta_0^2+\theta_1^2 = -3$ thus

$$31^2\theta_0\theta_1 + 31\cdot 9(\theta_0^2+\theta_1^2) + 9^2\theta_1\theta_0 = 2(31^2+9^2) - 3\cdot 31\cdot 9$$
$$= 1247$$

which is consistent with the Python program. From the pattern above what we see is that when computing the norm we want to group the $f(\alpha^l)$ such that the total is λ, *i.e.*

$$f(\alpha^{l_1})f(\alpha^{l_2})\dots f(\alpha^{l_n})$$

where $l_1+l_2+\cdots+l_n = \lambda$.

Page 87, Problem 6. We need to show that if $f(\alpha) = g(\alpha)$ then $f(1) \equiv g(1) \mod \lambda$. This is quite straightforward. If $f(\alpha) = g(\alpha)$ then their difference must be of the form $c(1+\alpha+\cdots+\alpha^{\lambda-1})$. Therefore

$$h(\alpha) = f(\alpha) - g(\alpha) = c(1+\alpha+\cdots+\alpha^{\lambda-1})$$
$$\rightarrow h(1) = (1+1+\cdots+1) = \lambda$$

since there are exactly λ terms in the bracket.

The second part asks you to show that $Nf(\alpha) \equiv 0$ or $1 \mod \lambda$. It took longer than it should because I made the unnecessary assumption about something LOL

We need to utilize the above result, $f(\alpha) = g(\alpha) \rightarrow f(1) \equiv g(1) \mod \lambda$. This one is easy enough, let $f(\alpha)$ be $Nf(\alpha)$ and $g(\alpha) = f(\alpha)f(\alpha^2)\dots f(\alpha^{\lambda-1})$ and so we have

$$[Nf](1) \equiv f(1)f(1^2)\dots f(1^{\lambda-1}) \mod \lambda$$
$$\equiv f(1)f(1)\dots f(1) \mod \lambda$$
$$\equiv \{f(1)\}^{\lambda-1} \mod \lambda$$

but by Fermat's Little Theorem and the fact that λ is prime we have $\{f(1)\}^{\lambda-1} \equiv 1 \mod \lambda$ unless when $f(1) \equiv 0 \mod \lambda$.

The task now is to show that $[Nf](\alpha) \equiv [Nf](1) \mod \lambda$. For this we utilize the result from Page 83 that says $[Nf](\alpha) = b_0 + b_1\alpha + \cdots + b_{\lambda-1}\alpha^{\lambda-1}$ with $b_1 = b_2 = \cdots = b_{\lambda-1}$ and so $[Nf](\alpha) = b_0 - b_1$.

Therefore $[Nf](\alpha) = b_0 + b_1(\alpha + \cdots + \alpha^{\lambda-1})$, we now need to use the usual trick $-1 = \alpha + \cdots + \alpha^{\lambda-1}$ and write $b_0 = -b_0(\alpha + \cdots + \alpha^{\lambda-1})$ and so

$$\begin{aligned} [Nf](\alpha) &= (b_1 - b_0)(\alpha + \cdots + \alpha^{\lambda-1}) \\ \rightarrow [Nf](1) &= (b_1 - b_0)(\lambda - 1) \end{aligned}$$

but $b_1 - b_0 = -[Nf](\alpha)$ thus

$$\begin{aligned} [Nf](1) &= [Nf](\alpha) - \lambda[Nf](\alpha) \\ \rightarrow [Nf](1) &\equiv [Nf](\alpha) \mod \lambda \end{aligned}$$

combining this with our previous result we get

$$\begin{aligned} [Nf](\alpha) \equiv [Nf](1) &\equiv \{f(1)\}^{\lambda-1} \mod \lambda \\ &\equiv 0 \text{ or } 1 \mod \lambda \end{aligned}$$

The reason I got stuck was somehow I felt that when setting $[Nf](\alpha) \rightarrow [Nf](1)$ we cannot do it by setting $f(1)f(1^2)\ldots f(1^{\lambda-1})$, so setting $\alpha = 1$ and then multiplying the f's would be different from multiplying the f's and then setting $\alpha = 1$. But of course this is not true, because 1 behaves just like α, $1^\lambda = 1$ so we can multiply them first and then set $\alpha = 1$ or set it to one first and then multiply (I believe you can do the same with zero as well as $0^\lambda = 1$).

Here I put square brackets around $[Nf]$ to differentiate between setting $\alpha = 1$ and then taking the norm of f and taking the norm of f and then setting $\alpha = 1$.

Page 87, Problem 7. Here we need to show that $f(\alpha)+f(\alpha^2)+\cdots+f(\alpha^{\lambda-1}) \equiv -f(1) \mod \lambda$. The hint tells us to explicitly compute $f(1) + f(\alpha) + f(\alpha^2) + \cdots + f(\alpha^{\lambda-1})$. Note that this sum includes $f(1)$ unlike the problem statement which starts with $f(\alpha)$.

So we shall follow the hint. But instead of writing everything out let's pick a term from $f(\alpha)$, for example let's pick $b_i\alpha^i$. Changing $\alpha \to \alpha^j$ for each $j = 0, 1, 2, \ldots, \lambda - 1$ we get

$$\begin{aligned} b_i\alpha^i &\to b_i + b_i(\alpha^i + \alpha^{2i} + \cdots + \alpha^{(\lambda-1)i}) \\ &= b_i + b_i(\alpha + \alpha^2 + \cdots + \alpha^{(\lambda-1)}) \\ &= b_i + b_i(-1) = 0 \end{aligned}$$

Going to the second line we used the fact that since λ is prime the set $\{i, 2i, \ldots, (\lambda-1)i\}$ is equal to the set of remainders of λ sans 0. The above is true as long as $i \neq 0$ obviously as b_0 remains b_0 for all $f(\alpha^k)$ and the sum is

$$\begin{aligned} f(1) + f(\alpha) + \cdots + f(\alpha^{\lambda-1}) &= \lambda b_0 \\ &\equiv 0 \mod \lambda \end{aligned}$$

Thus we are done :) Except that we need to show that this also answers first part of Problem 6. This is simple, if $f(\alpha) = g(\alpha)$ then

$$f(\alpha) + \cdots + f(\alpha^{\lambda-1}) = g(\alpha) + \cdots + g(\alpha^{\lambda-1})$$

note that we exclude $f(1)$ and $g(1)$ this time, but the LHS is $\equiv -f(1) \mod \lambda$ and the RHS is $\equiv -g(1) \mod \lambda$ so we practically have $f(1) \equiv g(1) \mod \lambda$ in a more roundabout way :)

Page 87, Problem 8. We need to show that if $g(\alpha)$ is a conjugate of $f(\alpha)$ and $h(\alpha)$ is a conjugate of $g(\alpha)$ then $h(\alpha)$ is a conjugate of $f(\alpha)$.

Following the hint, a conjugation takes $\alpha \to \alpha^j$ where $\lambda \nmid j$. This means that $g(\alpha) = f(\alpha^j)$ and $h(\alpha) = g(\alpha^i) = f(\alpha^{ji})$. But since $\lambda \nmid i, j$ individually the product ij is also not a multiple of λ, thus $h(\alpha)$ is a conjugate of $f(\alpha)$.

The next part asks us to show that if $g(\alpha)$ is a conjugate of $f(\alpha)$ then $f(\alpha)$ is a conjugate of $g(\alpha)$. Again, here $g(\alpha) = f(\alpha^j)$ but since λ is prime there's an inverse of j such that $ij \equiv 1 \mod \lambda$, thus substituting $\alpha \to \alpha^i$ we get $g(\alpha^i) = f(\alpha^{ij}) = f(\alpha)$ and we are done.

Page 87, Problem 9.Here we want to strengthen result of Problem 6. If we restrict $f(\alpha) = A\alpha^j + B\alpha^k$ then not only that $Nf(1) \equiv 0$ or $1 \mod \lambda$ but also that every prime factor of $Nf(\alpha)$ is 0 or $1 \mod \lambda$.

Following the hint, we know that (without loss of generality assume $j < k$)

$$\begin{aligned} A\alpha^j + B\alpha^k &= \alpha^j(A + B\alpha^k) \\ \rightarrow N(A\alpha^j + B\alpha^k) &= N(\alpha^j) \cdot N(A + B\alpha^k) \\ &= 1 \cdot N(A + B\alpha) \end{aligned}$$

but

$$\begin{aligned} N(A + B\alpha) &= (A + B\alpha)(A + B\alpha^2)\dots(A + B\alpha^{\lambda-1}) \\ \rightarrow (A + B)N(A + B\alpha) &= (A + B)(A + B\alpha)(A + B\alpha^2)\dots(A + B\alpha^{\lambda-1}) \\ &= A^\lambda + B^\lambda \end{aligned}$$

which is the main theme of this chapter, *i.e.* the factorization of $x^n + y^n$ using roots of 1, see Page 76. But since λ is prime and therefore odd we can factorize

$$\begin{aligned} (A + B)N(A + B\alpha) = A^\lambda + B^\lambda &= (A + B)(A^{\lambda-1} - A^{\lambda-2}B + \dots + B^{\lambda-1}) \\ \rightarrow N(A + B\alpha) = Nf(\alpha) &= A^{\lambda-1} - A^{\lambda-2}B + \dots + B^{\lambda-1} \end{aligned}$$

because $f(\alpha)$ is a unit times a conjugate of $A + B\alpha$ as shown above. Now comes the main trick. First, say p is a prime factor of $Nf(\alpha)$ then

$$A^{\lambda-1} - A^{\lambda-2}B + \dots + B^{\lambda-1} \equiv 0 \mod p$$

but since $\gcd(A, B) = 1$ none of them is divisible by p because if one is then the other one must be also nullifying the co-primeness condition. This means that both A and B have inverses mod p. We can choose either A or B for the next step, here I will choose B. From the equivalence relation mod p above do the following

$$\begin{aligned} A^{\lambda-1} &\equiv -(-A^{\lambda-2}B + \dots + B^{\lambda-1}) \mod p \\ \rightarrow B^{-1}A^{\lambda-1} &\equiv -(-A^{\lambda-2}B^{-1}B + \dots + B^{-1}B^{\lambda-1}) \mod p \\ &\equiv -(-A^{\lambda-2}(-1) + \dots + B^{\lambda-2}) \mod p \end{aligned}$$

we now move $A^{\lambda-2}$ from RHS back to the LHS and repeat the process multiplying the whole thing by B^{-1} again

$$\begin{aligned} B^{-1}A^{\lambda-1} &\equiv -(-A^{\lambda-2} + \cdots + B^{\lambda-2}) \mod p \\ B^{-1}A^{\lambda-1} - A^{\lambda-2} &\equiv -(A^{\lambda-3}B + \cdots + B^{\lambda-2}) \mod p \\ \rightarrow B^{-2}A^{\lambda-1} - B^{-1}A^{\lambda-2} &\equiv -(A^{\lambda-3}B^{-1}B + \cdots + B^{-1}B^{\lambda-2}) \mod p \end{aligned}$$

and now the $A^{\lambda-3}$ term on the RHS is free of B and we can move it back to the LHS and after doing this $\lambda - 1$ times we get

$$\begin{aligned} B^{-(\lambda-1)}A^{\lambda-1} - B^{-(\lambda-2)}A^{\lambda-2} + \cdots + 1 &\equiv 0 \mod p \\ \rightarrow k^{\lambda-1} - k^{\lambda-2} + \cdots + 1 &\equiv 0 \mod p \end{aligned}$$

and here $k \equiv B^{-1}A$, had we chosen to use A^{-1} we would've gotten $k = BA^{-1}$. We now do the trick we always do when dealing with a geometric series. Multiply the whole thing by k and then add them up

$$\begin{aligned} k \times (1 - k + k^2 - \cdots + k^{\lambda-1}) &\equiv k - k^2 + k^3 - \cdots + k^{\lambda} \equiv 0 \mod p \\ \rightarrow (1 + k) \times (1 - k + k^2 - \cdots + k^{\lambda-1}) &\equiv 1 + k^{\lambda} \equiv 0 \mod p \end{aligned}$$

since λ is odd it's either $k \equiv -1$ or $k^{\lambda} \equiv -1 \mod p$. But if $k \equiv -1$ then we have

$$\begin{aligned} 1 - k + k^2 - \cdots + k^{\lambda-1} = 1 + 1 + 1 + \cdots + 1 &\equiv 0 \mod p \\ \rightarrow \lambda &\equiv 0 \mod p \end{aligned}$$

but since both λ and p are both prime the only possibility is that $p = \lambda$ and in that case $p \equiv 0 \mod \lambda$ which is the first result we need.

If $k^{\lambda} \equiv -1 \mod p$ then $k^{2\lambda} \equiv 1 \mod p$. Since 2 and λ are prime, the order (or exponent) of k must be either 2, λor 2λ and each must divide $p-1$ according to Fermat's Little Theorem. for the cases of the order being λ or 2λ this means that $\lambda | p-1$ or $2\lambda | p-1$, either way this means that $p - 1 \equiv 0 \mod \lambda$.

If the order of k is 2 then k can only be $+1$ or -1 (as $x^2 \equiv 1$ can only have two solutions). But $k \equiv -1$ is already covered above resulting in $p \equiv 0 \mod \lambda$ and as shown above $1 + k^{\lambda} \equiv 0 \mod p$ which means that k cannot be 1.

Page 87, Problem 10. We want to show that $\alpha^{\lambda-1}$ is the complex conjugate of α. This is straightforward enough. From the definition of complex conjugation and the fact that α is a root of unity, we have

$$|\alpha|^2 = \alpha\ \overline{\alpha} = 1$$

but we also have $\alpha^{\lambda} = \alpha \cdot \alpha^{\lambda-1} = 1$, equating the two we get $\overline{\alpha} = \alpha^{\lambda-1}$. This also means that the complex conjugate of α^j is given by $\alpha^{\lambda-j}$.

Now we need to fill in the holes in the proof that $Nf(\alpha) \geq 0$ on (bottom part of) Page 83. There's not a lot to fill in actually except that $f(\alpha^j) = 0$ for some, and hence for all, $j = 1, 2, \ldots, \lambda - 1$.

The other steps are obvious

$$\begin{aligned} Nf(\alpha) &= f(\alpha)f(\alpha^2)\ldots f(\alpha^{\lambda-2})f(\alpha^{\lambda-1}) \\ &= f(\alpha)f(\alpha^2)\ldots f(\overline{\alpha^2})f(\overline{\alpha}) \\ &= f(\alpha)f(\alpha^2)\ldots \overline{f(\alpha^2)}\ \overline{f(\alpha)} \\ &= |f(\alpha)|^2|f(\alpha^2)|^2\ldots|f(\alpha^{\frac{\lambda-1}{2}})|^2 \end{aligned}$$

note that since λ is an odd prime $\lambda - 1$ is even. Now we need to show that if $f(\alpha^j) = 0$ for some j then it is zero for all j. This is also straightforward from the fact that $0 = c(1 + \alpha + \cdots + \alpha^{\lambda-1})$ thus if $f(\alpha^j) = 0$ then it must be of the form $c(1 + \alpha + \cdots + \alpha^{\lambda-1})$, but any conjugation of this form is also of this form since λ is prime and a (non-zero) multiple of the unit group of λ gives back the unit group $(\mathbb{Z}/\lambda\mathbb{Z})^*$.

Page 87, Problem 11. Here we want to divide a cyclotomic integer by another one for $\lambda = 5$. We want the quotient of $38\alpha^3 + 62\alpha^2 + 56\alpha + 29$ divided by $3\alpha^3 + 4\alpha^2 + 7\alpha + 1$. Again, here I'll write a Python script which would be an extension of the on in Problem 5. The method is to do the following

$$\begin{aligned} h(\alpha)g(\alpha) &= f(\alpha) \\ \rightarrow (Nh(\alpha))g(\alpha) &= f(\alpha)h(\alpha^2)h(\alpha^3)\ldots h(\alpha^{\lambda-1}) \\ \rightarrow g(\alpha) &= \frac{1}{Nh(\alpha)} f(\alpha)h(\alpha^2)h(\alpha^3)\ldots h(\alpha^{\lambda-1}) \end{aligned}$$

to be able to divide the whole thing on the RHS by $Nh(\alpha)$ we might need to massage the product $f(\alpha)h(\alpha^2)h(\alpha^3)\ldots h(\alpha^{\lambda-1})$ such that every coefficient is divisible by $Nh(\alpha)$, we

can do this provided each coefficient has the same number modulo $Nh(\alpha)$ as explained on Page 85.

```
# do division f/h
def divCyc(f, h):

    if len(f) != len(h):
        return

    L = len(f)

    if L == 1:
        return [f[0]/h[0]]

    Nh = cycNorm(h)

    res = [i for i in f] # deep copy of f
    for k in xrange(2,L):
        hk = cycShift(h, k)
        res = multCyc(res, hk)

    # check if every coefficient is the same modulo Nh
    for k in xrange(1,L):
        if (res[k] % Nh) != (res[k-1] % Nh):
            return

    # now subtract the higest coefficient from each coefficient and divide by Nh
    for k in xrange(L):
        res[k] = (res[k] - res[-1])/Nh

    return res
```

and for our particular problem at hand the answer is $-7\alpha^3 - 3\alpha^2 - \alpha + 2$.

Page 87, Problem 12. We need to prove that $f(\alpha)$ is divisible by $\alpha - 1$ if and only if $f(1) \equiv 0 \mod \lambda$. One direction is easy, if $f(\alpha)$ is divisible by $\alpha - 1$ then $f(\alpha) = (\alpha - 1)h(\alpha)$, setting $\alpha \to 1$ we get 0 and therefore $\equiv 0 \mod \lambda$.

The other direction not so much :) but we can learn something from the other direction. If $f(\alpha)$ is divisible by $\alpha - 1$ then

$$\begin{aligned} f(\alpha) = (\alpha - 1)h(\alpha) &= (\alpha - 1)(c_0 + c_1\alpha + \cdots + c_{\lambda-1}\alpha^{\lambda-1}) \\ &= (c_{\lambda-1} - c_0) + (c_0 - c_1)\alpha + (c_1 - c_2)\alpha^2 + \cdots + (c_{\lambda-2} - c_{\lambda-1})\alpha^{\lambda-1} \end{aligned}$$

while on the other hand

$$f(\alpha) = b_0 + b_1\alpha + \cdots + b_{\lambda_1}\alpha^{\lambda-1}$$

$$\to 0 \mod \lambda \equiv f(1) = \lambda m = b_0 + b_1 + \cdots + b_{\lambda_1}$$

$$\to f(\alpha) = (b_0 - m) + (b_1 - m)\alpha + \cdots + (b_{\lambda_1} - m)\alpha^{\lambda-1}$$

which is saying that since there are λ m's we can spread them to the λ coefficients of $f(\alpha)$ and in so doing $f(1)$ is now exactly 0.

Our task now is to show that given such $f(\alpha) = (b_0-m)+(b_1-m)\alpha+\cdots+(b_{\lambda_1}-m)\alpha^{\lambda-1}$, it is possible to find λ coefficients $c_0, c_1, \ldots, c_{\lambda-1}$ such that $c_{\lambda-1} - c_0 = b_0 - m, c_0 - c_1 = b_1 - m, \ldots, c_{\lambda-2} - c_{\lambda-1} = b_{\lambda-1} - m$ and thus $h(\alpha) = c_0 + c_1\alpha + \cdots + c_{\lambda-1}\alpha^{\lambda-1}$ and $h(\alpha)(\alpha - 1) = f(\alpha)$.

Staring at this problem long enough you'll see that the key to success is determined by setting $c_{\lambda-1} = 0$ and the rest will follow. Let's see it work, setting $c_{\lambda-1} = 0$ we get

$$\begin{aligned} c_{\lambda-2} &= b_{\lambda-1} - m \\ c_{\lambda-3} - c_{\lambda-2} &= b_{\lambda-2} - m \\ &\vdots \\ c_0 - c_1 &= b_1 - m \\ -c_0 &= b_0 - m \end{aligned}$$

so by setting $c_{\lambda-1} = 0$ we are practically setting the solution for all c's from both ends, from $c_{\lambda-2}$ going down and from c_0 going up, the only question now is whether we will get a consistent result coming from both ends.

The answer is yes, here's why, the easiest way to see this is to start from the top all the way to the bottom and see if we can get $-c_0 = b_0 - m$. If we add everything starting from the top

$$\begin{aligned} c_{\lambda-2} &= b_{\lambda-1} - m \\ c_{\lambda-3} - c_{\lambda-2} &= b_{\lambda-2} - m \\ &\vdots \\ c_0 - c_1 &= b_1 - m \\ \hline \qquad + \qquad \hline \qquad + \\ c_0 &= \textstyle\sum_{i=1}^{\lambda-1} b_i - m(\lambda-1) \end{aligned}$$

but we know that $f(1) = 0 = \sum_{i=0}^{\lambda-1} b_i - m\lambda$ this means that $\sum_{i=1}^{\lambda-1} b_i - m(\lambda-1) = -(b_0-m)$ and thus $-c_0 = b_0 - m$ which is consistent with our previous result above. The same can be said if we go from the bottom to the top but actually we can even start from both

ends and stop anywhere we want in the middle and the result will still be consistent by just summing both sides like above. This also serves as a good way to calculate division by $\alpha - 1$.

Thus if $f(1) \equiv 0 \mod \lambda$ then $f(\alpha)$ is divisible by $\alpha - 1$. We now need to show that this also serves as a proof of the first half of Problem 6. If $\alpha - 1$ divides $f(\alpha)$ then from $f(\alpha) = g(\alpha)$, $\alpha - 1$ also divides $g(\alpha)$ therefore $f(1) \equiv 0$ and $g(1) \equiv 0 \mod \lambda$ and therefore $0 \equiv f(1) \equiv g(1) \mod \lambda$.

But say $\alpha - 1$ does not divide $f(\alpha)$ which means that it doesn't divide $g(\alpha)$ either, this means that $f(1) \equiv k_f \mod \lambda$ and $g(1) \equiv k_g \mod \lambda$, this means that $f(\alpha) - k_f$ and $g(\alpha) - k_g$ are both divisible by $\alpha - 1$. But $f(\alpha) = g(\alpha)$ which means that $f(\alpha) - k_g$ is divisible by $\alpha - 1$ and therefore $f(1) - k_g \equiv 0 \mod \lambda$ but we also have $f(1) - k_f \equiv 0 \mod \lambda$, this means that $0 \equiv f(1) - k_g \equiv f(1) - k_f \mod \lambda$ which also means that $k_g \equiv k_f \mod \lambda$ which lastly means that $f(1) \equiv g(1) \mod \lambda$ since $f(1) \equiv k_f$ and $g(1) \equiv k_g \mod \lambda$.

We can also show this by simply noting that if $f(\alpha) = g(\alpha)$ then $h(\alpha) = f(\alpha) - g(\alpha) = 0$, therefore $(\alpha - 1)|h(\alpha)$, since $h(\alpha) = 0$ is divisible by anything :) Using the result of Problem 12, divisibility by $\alpha - 1$ means we have $h(1) = f(1) - g(1) \equiv 0 \mod \lambda \rightarrow f(1) \equiv g(1) \mod \lambda$. Yet another proof of Problem 6.

The third and last part of this problem asks us to divide both cyclotomic integers in Problem 11 by $\alpha - 1$. This time I will do it by hand instead of a Python script because we can do it quite easily using the method we discovered above, *i.e.*

1. Calculate $f(1)$, in this case it will be $f(1) = \lambda m$ since $f(\alpha)$ is divisible by $\alpha - 1$.

2. Transform $f(\alpha)$ from $b_0 + b_1\alpha + \cdots + b_{\lambda-1}\alpha^{\lambda-1}$ to $(b_0 - m) + (b_1 - m)\alpha + \cdots + (b_{\lambda-1} - m)\alpha^{\lambda-1}$.

3. From $(\alpha - 1)h(\alpha) = f(\alpha)$ we know that $(c_{\lambda-1} - c_0) = b_0 - m, (c_1 - c_0) = b_1 - m, \ldots, (c_{\lambda-2} - c_{\lambda-1}) = b_{\lambda-1} - m$.

Set $c_{\lambda-1} = 0$ and we get the full solution for all c's where $h(\alpha) = c_0 + c_1\alpha + \cdots + c_{\lambda-1}\alpha^{\lambda-1}$.

Let's do it for $f(\alpha) = 38\alpha^3 + 62\alpha^2 + 56\alpha + 29$, here $f(1) = 185$ thus with $\lambda = 5$ we

have $m = 37$. Transform $f(\alpha)$ into $-37\alpha^4 + \alpha^3 + 25\alpha^2 + 19\alpha - 8$, setting $c_4 = 0$ we get

$$\begin{aligned} c_3 - c_4 &= -37 \rightarrow c_3 = -37 \\ c_2 - c_3 &= 1 \quad \rightarrow c_2 = -36 \\ c_1 - c_2 &= 25 \quad \rightarrow c_1 = -11 \\ c_0 - c_1 &= 19 \quad \rightarrow c_0 = 8 \\ c_4 - c_0 &= -8 \quad \rightarrow c_0 = 8 \end{aligned}$$

the last one was just a consistency check. Thus $h(\alpha) = \frac{f(\alpha)}{\alpha - 1} = -37\alpha^3 - 36\alpha^2 - 11\alpha + 8$.

For the other cyclotomic number $f(\alpha) = 3\alpha^3 + 4\alpha^2 + 7\alpha + 1$ we have $f(1) = 15$ thus $m = 3$, we then transform $f(\alpha)$ into $-3\alpha^4 + 0\alpha^3 + \alpha^2 + 4\alpha - 2$, setting $c_4 = 0$ we get

$$\begin{aligned} c_3 - c_4 &= -3 \rightarrow c_3 = -3 \\ c_2 - c_3 &= 0 \quad \rightarrow c_2 = -3 \\ c_1 - c_2 &= 1 \quad \rightarrow c_1 = -2 \\ c_0 - c_1 &= 4 \quad \rightarrow c_0 = 2 \\ c_4 - c_0 &= -2 \rightarrow c_0 = 2 \end{aligned}$$

And the answer this time is $h(\alpha) = \frac{f(\alpha)}{\alpha - 1} = -3\alpha^3 - 3\alpha^2 - 2\alpha + 2$.

Page 87, Problem 13. We choose two cyclotomic integers at random, multiply them and then use the division algorithm, we do this first for $\lambda = 5$ then for $\lambda = 7$. The script to generate the random cyclotomic integers is as follows

```
# generate random cyclotomic integers
def randCyc(L):
    import random as rand

    rand.seed()

    return [rand.randint(-100,100) for i in xrange(L)]
```

The rest of the python script to multiple and divide cyclotomic integers is available at problem 5 and Problem 11. Running the above script I got the following cyclotomic

integers for $\lambda = 5$

$$\begin{aligned} A &= 46\alpha^4 - 95\alpha^3 + 53\alpha^2 + 44\alpha - 39 \\ B &= 77\alpha^4 - 57\alpha^3 - 18\alpha^2 - 76\alpha - 80 \\ AB &= -2925\alpha^4 + 8545\alpha^3 - 16819\alpha^2 + 8112\alpha + 1701 \\ (AB)/A &= -134\alpha^3 - 95\alpha^2 - 153\alpha - 157 \\ (AB)/B &= -141\alpha^3 + 7\alpha^2 - 2\alpha - 85 \end{aligned}$$

and for $\lambda = 7$ I got

$$\begin{aligned} A &= 27\alpha^6 + 36\alpha^5 + 63\alpha^4 + 35\alpha^3 + 19\alpha^2 - 42\alpha + 46 \\ B &= 36\alpha^6 + 62\alpha^5 + 99\alpha^4 + 80\alpha^3 - 66\alpha^2 - 70\alpha - 91 \\ AB &= -488\alpha^6 - 2258\alpha^5 + 6193\alpha^4 + 15480\alpha^3 + 12523\alpha^2 + 3147\alpha + 8091 \\ (AB)/A &= 26\alpha^5 + 63\alpha^4 + 44\alpha^3 - 102\alpha^2 - 106\alpha + 55 \\ (AB)/B &= 9\alpha^5 + 36\alpha^4 + 8\alpha^3 - 8\alpha^2 - 69\alpha + 19 \end{aligned}$$

Page 88, Problem 14. We need to show that if $f(\alpha)g(\alpha) = 1$ then $f(\alpha)$ is a unit and $g(\alpha) = f(\alpha^2)f(\alpha^3)\dots f(\alpha^{\lambda-1})$. We just follow the hint.

Take the norm

$$Nf(\alpha)\ Ng(\alpha) = 1$$

since the norm is a non-negative integer both $Nf(\alpha) = Ng(\alpha) = 1$ which means that $f(\alpha)$ is a unit. This also means that

$$\begin{aligned} 1 = f(\alpha)g(\alpha) &= Nf(\alpha) \\ &= f(\alpha)f(\alpha^2)f(\alpha^3)\dots f(\alpha^{\lambda-1}) \\ \rightarrow g(\alpha) &= f(\alpha^2)f(\alpha^3)\dots f(\alpha^{\lambda-1}) \end{aligned}$$

Now the question is can there be other options for $g(\alpha)$? Say $g(\alpha) = h(\alpha) \neq f(\alpha^2)f(\alpha^3)\dots f(\alpha^{\lambda-1})$ then we will have a contradiction

$$\begin{aligned} 1 = f(\alpha)g(\alpha) &= Nf(\alpha) \\ f(\alpha)h(\alpha) &= f(\alpha)f(\alpha^2)f(\alpha^3)\dots f(\alpha^{\lambda-1}) \\ \rightarrow h(\alpha) &= f(\alpha^2)f(\alpha^3)\dots f(\alpha^{\lambda-1}) \end{aligned}$$

Also, this means that $f(\alpha) = g(\alpha^2)g(\alpha^3)\dots g(\alpha^{\lambda-1})$.

Page 88, Problem 15. Here we need to fill in the gaps and details of the proof that there is no other relation $f(\alpha) = 0$ than the one shown in the book $c(1 + \alpha + \alpha^2 + \cdots + \alpha^{\lambda-1}) = 0$.

For the middle steps, when it says "If $r(X) \neq 0$ replace $f(X)$ by $r(X)$ and repeat the process." What it means is that we initially assume that there's a polynomial $f(X)$ of degree less than $\lambda - 1$ where $f(\alpha) = 0$.

We then do the $x = by + r$ trick $ah(X) = q(X)f(X) + r(X)$, since $h(\alpha) = 0 = f(\alpha)$ this means that $r(\alpha) = 0$ as well. But $r(X)$ being the remainder has a degree even less than $f(X)$. Since this is the case we move from examining $f(X)$ to examining $r(X)$. We then repeat the process $ah(X) = q(X)r(X) + r'(X)$ but by the same argument we have $r'(\alpha) = 0$ and $r'(X)$ having an even lesser degree than $r(X)$.

But we need to be careful because sometimes we cannot get the remainder to have a degree lesser than that of the divisor. Therefore we need to allow rational numbers in the quotient and remainder and then multiply the whole thing by the common denominator For example if we divide $X^2 + X + 1$ by $12X + 17$, first we need to multiply $X^2 + X + 1$ by 12, but even after we do this to get a remainder with a lesser degree than the divisor's we need to include rationals like so

$$\begin{aligned} 12(X^2 + X + 1) &= (12X + 17)(X + \tfrac{5}{12}) + (\tfrac{59}{12}) \\ \Rightarrow\ 12 \cdot 12(X^2 + X + 1) &= (12X + 17)(12X + 5) + (59) \end{aligned}$$

and at the end we multiply the whole thing by 12 to get $a = 144$, $f(X) = 12X + 17$, $q(X) = 12X + 5$ and $r(X) = 59$. If we did not include rationals the remainder would be $-5X + 12$ which is the same degree as the divisor and the cycle might not terminate.

But once we get the remainder to be just a constant we can stop because $ah(X) = f(X)q(X) + r(X)$ means that since $h(\alpha) = 0$ and $f(\alpha) = 0$ we must have $r(\alpha) = 0$. If $r(X)$ is a non-zero constant then we are done because we already have our contradiction. If $r(X) = 0$ then we move on to the next step of the proof where we only consider $f(X)$ that divides $ah(X)$.

Next is the statement that "$h(j) \equiv 1 \mod \lambda$ for $j \not\equiv 1 \mod \lambda$". We use the geometric series formula $1 + j + \cdots + j^{\lambda-1} = \frac{j^\lambda - 1}{j-1}$, since $j \not\equiv 1$ there's nothing wrong with dividing

by $j-1$. Now assume that this value is A

$$\frac{j^\lambda - 1}{j-1} \equiv A \mod \lambda$$

but by Fermat's Little Theorem $j^\lambda \equiv j^{\lambda-1} \cdot j \equiv 1 \cdot j \mod \lambda$ thus

$$\frac{j^\lambda - 1}{j-1} \equiv \frac{j-1}{j-1} \equiv 1 \equiv A \mod \lambda$$

and $1 + j + \cdots + j^{\lambda-1} \equiv A \equiv 1 \mod \lambda$.

The next thing we need is "A polynomial $F(X)$ is divisible by $(X-1) \mod \lambda$ if and only if $F(1) \equiv 0 \mod \lambda$." The if part is easy enough to see, the only if part not so much. The way to see this is using the fundamental theorem of algebra applied to congruences or by the following, if $F(X)$ is a polynomial of degree $n \mod \lambda$ and $F(r) \equiv 0 \mod \lambda$ then

$$\begin{aligned} F(X) &\equiv F(X) - F(r) \\ &\equiv c_n(X^n - r^n) + c_{n-1}(X^{n-1} - r^{n-1}) + \cdots + c_0(1-1) \\ F(X) &\equiv (X-r)\left\{c_n(X^{n-1} + X^{n-2}r + \cdots + Xr^{n-2} + r^{n-1}) + \right. \\ &\qquad \left. c_{n-1}(X^{n-2} + X^{n-3}r + \cdots + Xr^{n-3} + r^{n-2}) + \cdots + c_1\right\} \end{aligned}$$

and thus this means that $(X-r)$ divides $F(X)$.

The next confusing thing is that "This is true for either $f(X)$or $g(X)$ but not both", the word "This" refers to divisibility by $(X-1)$. The way to see this is as follows, from $h(X) = f(X)g(X)$ set $X = 1$, since $h(X) = 1 + X + X^2 + \cdots + X^{\lambda-1}$ we have $h(1) = \lambda$ and $\lambda = f(1)g(1)$. But λ is prime thus it is either $f(1) = \lambda$ or $g(1) = \lambda$ but it can't be both. This also means that only one of these is true, $f(1) \equiv 0 \mod \lambda$ or $g(1) \equiv 0 \mod \lambda$, and using the theorem $F(X)$ divisible by $X-1$ if and only if $F(1) \equiv 0 \mod \lambda$ we can only have either $f(X)$ or $g(X)$ divisible by $X-1$ but not both.

Page 88, Problem 16. We need to prove by algebraic means that if $f(\alpha)h(\alpha) = g(\alpha)h(\alpha)$ then $f(\alpha) = g(\alpha)$. Now the hint says that we just need to consider the case $g(\alpha) = 0$. Why? The key point is this, first let $g(\alpha) = 0$ then we have $f(\alpha)h(\alpha) = 0$, but it need not mean that $f(\alpha) = 0$ it may mean that the product $f(\alpha)h(\alpha) = 0$ but not the individual numbers.

If $g(\alpha) \neq 0$ we just need to do the following substitution $f(\alpha) \to f(\alpha) - g(\alpha)$ and $g(\alpha) \to 0$ like before and we have

$$(f(\alpha) - g(\alpha))h(\alpha) = 0$$

if we prove the theorem for the case $g(\alpha) = 0$ this means that in this case $f(\alpha) - g(\alpha) = 0$ and therefore $f(\alpha) = g(\alpha)$.

The hint tells us to us the argument in Problem 15. But we must use it in a different way. Here we are not trying to express $al(X)$ as $f(X)h(X)$ this is because $f(X)$ and $h(X)$ can now be of order $\lambda - 1$ each giving a total order of $2(\lambda - 1)$. (Note the notation change since $h(\alpha)$ is already used, so now we use $l(X) = X^{\lambda-1} + X^{\lambda-2} + \cdots + 1$).

We can still continue with it if we want to but then the LHS is no longer $al(X)$ instead it must be a generic polynomial of degree $2(\lambda - 1)$ that is zero when $X = \alpha$, *i.e.*

$$al(X)(c_1X^{\lambda-1} + c_2X^{\lambda-2} + \cdots + c_\lambda) = f(X)h(X) + r(X)$$

The problem with this is that when we arrived at the step where $X - 1$ divides $f(X)$ or $h(X)$ but not both we can't assert the same thing anymore. This is because previously $l(1) = \lambda = f(1)h(1)$ but now we have

$$\lambda(c_1 + c_2 + \cdots + c_\lambda) = f(1)h(1)$$

and the sum of the coefficients can still be a multiple of λ therefore both $f(1)$ and $h(1)$ can both be a multiple of $X - 1$ and we can't have the same contradiction as before.

The right way to do it is the following. Set $al(X) = f(X)q(X) + r(X)$ where $f(\alpha)h(\alpha) = 0$ and $r(\alpha)h(\alpha) = 0$. Just like before each $r(X)$ can be made to have a lower degree than that of the divisor and we repeat the process until we reach a zero $r(X)$ or a constant one.

If $r(X) = k$ is a non-zero constant then $kh(\alpha) = 0$ which means that $h(\alpha) = 0$ a contradiction since it was assumed that $h(\alpha) \neq 0$. If $r(X) = 0$ then we have an $f(X)$ that divides $l(X)$ and the proof continues like the one in Problem 15.

The final conclusion is slightly different, the assumption that there is a non-zero $f(\alpha)$ that has a product with $h(\alpha) \to f(\alpha)h(\alpha) = 0$ leads to a contradiction, therefore $f(\alpha) = 0 = g(\alpha)$. The lesson here is that

1. No matter what we need to keep the LHS of $al(X) = f(X)q(X) + r(X)$ to be a polynomial of degree $\lambda - 1$ to ensure $l(1) = f(1)q(1) = \lambda$. This makes sure that only one of $f(X)$ or $q(X)$ is divisible by $X - 1$, otherwise the proof fails.

2. We need not have $f(\alpha)$ to be zero, we can have other conditions such as the one above $f(\alpha)h(\alpha) = 0$ or something else like $f(\alpha)h(\alpha)u(\alpha)$.

So the above two points are the gist of the proof of Problem 15.

Page 88, Problem 17. Here we need to show that the properties of congruences apply to cyclotomic integers. The first $h(\alpha) \equiv h(\alpha)$ one is straightforward since $h(\alpha) - h(\alpha) = 0$ and 0 is divisible by anything :)

The second one $h(\alpha) \equiv k(\alpha)$ implies $k(\alpha) \equiv h(\alpha)$ is also straightforward if

$$h(\alpha) \equiv k(\alpha) \mod f(\alpha) \rightarrow f(\alpha)u(\alpha) = h(\alpha) - k(\alpha) \rightarrow f(\alpha)(-u(\alpha)) = k(\alpha) - h(\alpha)$$

which means that $\rightarrow k(\alpha) \equiv h(\alpha) \mod f(\alpha)$. Next, transitivity, $h(\alpha) \equiv k(\alpha)$ and $k(\alpha) \equiv g(\alpha)$ means $h(\alpha) \equiv g(\alpha)$

$$\begin{aligned} h(\alpha) \equiv k(\alpha) \mod f(\alpha) &\rightarrow h(\alpha) - k(\alpha) = f(\alpha)u(\alpha) \\ k(\alpha) \equiv g(\alpha) \mod f(\alpha) &\rightarrow k(\alpha) - g(\alpha) = f(\alpha)v(\alpha) \end{aligned}$$

adding the two equalities we get

$$h(\alpha) - \cancel{k(\alpha)} + \cancel{k(\alpha)} - g(\alpha) = f(\alpha)(u(\alpha) + v(\alpha))$$

so $h(\alpha) \equiv g(\alpha) \mod f(\alpha)$. The last two are addition and multiplication, first, addition

$$\begin{aligned} h_1(\alpha) \equiv k_1(\alpha) \mod f(\alpha) &\rightarrow h_1(\alpha) = k_1(\alpha) + f(\alpha)u(\alpha) \\ h_2(\alpha) \equiv k_2(\alpha) \mod f(\alpha) &\rightarrow h_2(\alpha) = k_2(\alpha) + f(\alpha)v(\alpha) \end{aligned}$$

adding the two equalities we get what we want, lastly, multiplication, just multiply the two equalities to get

$$h_1(\alpha)h_2(\alpha) = k_1(\alpha)k_2(\alpha) + f(\alpha)\{k_1(\alpha)v(\alpha) + k_2(\alpha)u(\alpha) + u(\alpha)v(\alpha)\}$$

Page 88, Problem 18. We need to prove that a prime cyclotomic integer is irreducible. Assume the contrary, then a prime $p(\alpha)$ can be split into $p(\alpha) = f(\alpha)g(\alpha)$ where

f and g are not units, we also note that $p(\alpha)$ does not divide f nor g because if we take the norm

$$Np(\alpha) = Nf(\alpha)Ng(\alpha)$$

since the norm is a (non-zero) integer $Nf, Ng < Np$ and if $p(\alpha)$ divides f or g then

$$p(\alpha)u(\alpha) = f(\alpha)$$
$$\rightarrow Np(\alpha)Nu(\alpha) = Nf(\alpha)$$

which means that either $Np(\alpha) = Nf(\alpha)$ and in this case g is a unit contrary to our assumption about g or $Np(\alpha) < Nf(\alpha)$ which also is a contradiction. Thus $p(\alpha)$ does not divide f nor g, but $p(\alpha)$ certainly divides the product $f(\alpha)g(\alpha)$ since it is $p(\alpha)$ itself contrary to the definition of a prime cyclotomic integer where you have to divide the factors to divide the product to be a prime.

Page 88, Problem 19. Need to show that for ordinary integers, irreducible means prime. If an integer p is irreducible this means that $p = mn$ where m or n is a unit, *i.e.* plus minus 1. If m is a unit then n must be irreducible otherwise we can factor n and p is no longer irreducible. So if m is ± 1 then $n = \pm p$ but this is the very definition of a prime number.

Page 91, theorem at top of page, note that it is an if and only if so if we have $f(k) \equiv g(k) \mod p$ we also have $f(\alpha) \equiv g(\alpha) \mod h(\alpha)$ as long as $h(\alpha)$ is a prime that divides a binomial $x + \alpha^j y$.

Page 91, lower page, "$p = \lambda, h(\alpha)$ divides $\alpha - 1$ because $1 - 1 \equiv 0 \mod \lambda$". I found this logic to be a little faulty. The thing is just because $1 - 1 \equiv 0 \mod \lambda$ it doesn't mean that $\alpha - 1$ is divisible by $h(\alpha)$. If that's the case then we can use any number we want $7 - 7 \equiv 0 \mod \lambda$ therefore $\alpha - 7$ is divisible by $h(\alpha)$?

This is obviously not true, the thing is that $\alpha \equiv k$ also means that k must satisfy Eq (1) on Page 91, we of course know that $k = 1$ does therefore $\alpha - 1$ is divisible by $h(\alpha)$.

Page 91, last paragraph, $N(\alpha - 1) = N(1 - \alpha)$, this is because the norm is a product of $\lambda - 1$ terms and since λ is an odd prime $\lambda - 1$ is an even number, since the norm is a product of an even number of terms we have $N(f(\alpha)) = N(-f(\alpha))$.

Page 92, top of page "$\alpha \to \alpha^i$ preserve products", it doesn't mean that $w(\alpha)u(\alpha) = w(\alpha^i)u(\alpha^i)$. What it means is

$$w(\alpha)u(\alpha) = f(\alpha^j)g(\alpha^j)$$
$$\to w(\alpha^i)u(\alpha^i) = f(\alpha^{ij})g(\alpha^{ij})$$

Page 92, top of page "Also each divides a binomial and each divides p", the p refers to the same prime number, *i.e.* all conjugates $h(\alpha^j)$ of $h(\alpha)$ divides the same prime number p, this is because the previous explanation above if $h(\alpha)$ divides p then

$$h(\alpha)g(\alpha) = p$$
$$\to h(\alpha^j)g(\alpha^j) = p$$

like said above that "$\alpha \to \alpha^i$ preserve products". And the conjugates $h(\alpha^j)$ cannot divide other prime numbers due to the reason mentioned previously, if $h(\alpha^j)$ divides another prime q then $h(\alpha)$ also divides q by the argument above, and from Bezout's lemma we have $ap + bq = 1$ therefore $h(\alpha)$ divides 1 and it must be a unit and not a prime.

Page 92, top(ish) part of first paragraph, "two cyclotomic integers are congruent mod $h(\alpha^j)$ if and only if they are congruent mod $h(\alpha)$". This is because $h(\alpha)$ and $h(\alpha^j)$ share the same k and the same p and so we have (from Theorem on Page 91)

$$f(\alpha) \equiv g(\alpha) \mod h(\alpha) \iff f(k) \equiv g(k) \mod p \iff f(\alpha) \equiv g(\alpha) \mod h(\alpha^j)$$

Page 92, top(ish) part of first paragraph, "it follows that $h(\alpha^j)$ divides $h(\alpha)$ and $h(\alpha)$ divides $h(\alpha^j)$". To show this, first assume that $h(\alpha) \nmid h(\alpha^j)$ which can be written as $h(\alpha^j) \equiv g(\alpha) \mod h(\alpha)$ where $g(\alpha)$ can be anything.

Then from Page 91 Theorem we have $h(\alpha^j) \equiv g(\alpha) \mod h(\alpha) \iff h(k^j) \equiv g(k) \mod p$. But we also have $f(k) \equiv g(k) \mod p \iff f(\alpha) \equiv g(\alpha) \mod h(\alpha^j)$ since $h(\alpha^j)$ and $h(\alpha)$ share the same k and p. Therefore we have $h(k^j) \equiv g(k) \mod p \iff h(\alpha^j) \equiv g(\alpha) \mod h(\alpha^j)$. But $h(\alpha^j) \equiv 0 \mod h(\alpha^j)$ which means that $g(\alpha) \equiv 0 \mod h(\alpha^j)$.

And from $f(\alpha) \equiv g(\alpha) \mod h(\alpha) \iff f(k) \equiv g(k) \mod p \iff f(\alpha) \equiv g(\alpha) \mod h(\alpha^j)$ we have $g(\alpha) \equiv 0 \mod h(\alpha^j) \iff g(\alpha) \equiv 0 \mod h(\alpha)$. Finally our original statement $h(\alpha^j) \equiv g(\alpha) \mod h(\alpha)$ means that $h(\alpha^j) \equiv 0 \mod h(\alpha)$. If we start with $h(\alpha) \equiv g(\alpha) \mod h(\alpha^j)$ we will get the other result $h(\alpha) \equiv 0 \mod h(\alpha^j)$.

Page 92, mid of top paragraph. $\alpha^j \equiv k \equiv \alpha^i \mod \alpha^j$, note that in this case from the fact that $\alpha \equiv k \mod h(\alpha)$ we have $\alpha^j \equiv k \mod h(\alpha^j)$ for all j. We get $k \equiv \alpha^i \mod h(\alpha^j)$ because we have assumed that $h(\alpha^j)|h(\alpha^i)$.

Page 92, almost the end of big (top) paragraph, $q_{\lambda-1}(\alpha) = 1$, this is because $Nh(\alpha) = p$ because $h(\alpha)$ is a prime and thus not a unit.

Page 93, top page, proof of Theorems and Corollaries, the key ingredient here is $\alpha \equiv 1 \mod \alpha - 1$.

Page 93, top page, $f(\alpha)g(\alpha) \equiv 0 \mod \alpha - 1, f(1)g(1) \equiv 0 \mod \alpha - 1$, this is because $\alpha \equiv 1 \mod \alpha - 1$ so we can substitute 1 for α as long as it's mod $\alpha - 1$.

Page 93, end of first paragraph of proof, what we want to show is that a unit multiple of a prime cyclotomic is also a prime cyclotomic. We can prove this by contradiction. Say $q(\alpha)$ is prime and $p(\alpha) = u(\alpha)q(\alpha)$ is not. From the definition it's obvious that $p(\alpha)$ is irreducible.

Since $p(\alpha)$ is not prime there must be a number divisible by $p(\alpha)$ but whose factors are not divisible by $p(\alpha)$

$$p(\alpha)y(\alpha) = f(\alpha)g(\alpha)$$

but $p(\alpha) \nmid f(\alpha)$ and $p(\alpha) \nmid g(\alpha)$. However,

$$p(\alpha)y(\alpha) = q(\alpha)u(\alpha)y(\alpha) = f(\alpha)g(\alpha)$$

and $q(\alpha)|f(\alpha)$ or $q(\alpha)|g(\alpha)$, say in this case $q(\alpha)|f(\alpha)$ then

$$f(\alpha) = q(\alpha)F(\alpha)$$

but since a unit has an inverse, it divides everything so we can write $F(\alpha) = u(\alpha)\tilde{F}(\alpha)$ where $\tilde{F}(\alpha) = u^{-1}(\alpha)F(\alpha)$ therefore

$$\begin{aligned} f(\alpha) &= q(\alpha)u(\alpha)\tilde{F}(\alpha) \\ &= p(\alpha)\tilde{F}(\alpha) \end{aligned}$$

contrary to our assumption that $p(\alpha)$ doesn't divide $f(\alpha)$ thus a unit multiple of a prime is also a prime.

Page 93, mid(ish) of second paragraph of proof, "$\alpha - 1$ is the unique prime divisor of λ". From the previous paragraph we have that $\alpha^j - 1$ is a multiple of $\alpha - 1$ and $h(\alpha)$ and its conjugates are prime which are just unit multiples of conjugates of $\alpha - 1$.

Here $\lambda = Nh(\alpha)$ which is just a product of conjugates of $h(\alpha)$, each of which is prime and each of which is a unit multiple of $\alpha - 1$, thus $\lambda = Nh(\alpha)$ is just a product of a bunch of $\alpha - 1$ and a bunch of units and $\alpha - 1$ being the sole prime divisor of $\lambda = Nh(\alpha)$ although there might be multiple copies of it.

Page 93, mid(ish) of second paragraph of proof, "every conjugate of α is congruent to $1 \mod \alpha - 1$", this is because $\alpha \equiv 1 \mod \alpha - 1$ and thus $\alpha^j \equiv 1^j \equiv 1 \mod \alpha - 1$.

Page 93, last paragraph on the proof of second Theorem on Page 92, this proof uses the fact that $Nh(\alpha)$ is prime, I want to make it more general by assuming that $Nh(\alpha) = p^n$ a power of odd prime instead. This is because in the exercises we get something like $h(\alpha)$ divides a prime $p \equiv 1 \mod \lambda$ which implies that $Nh(\alpha)|p^j$ since $Np = p^{\lambda-1}$. However, we need not care too much about the norm because if $h(\alpha)|p$ with $p \equiv 1 \mod \lambda$ and $h(\alpha)$ is not a unit then it is a cyclotomic prime and divides a binomial.

Proposition 93.1, I use the page number as theorems in this book are not numbered, *If $Nh(\alpha) = p^n$ a power of odd prime, $n \geq 1$, and $p \equiv 1 \mod \lambda$, then $h(\alpha)$ divides a binomial, however, $h(\alpha)$ might not be prime except when $h(\alpha)|p$ then in that case $h(\alpha)$ is prime cyclotomic.*

Proposition 93.1.0, A reformulation of the above, *If a non-unit $h(\alpha)|p$ an odd prime and $p \equiv 1 \mod \lambda$, then $h(\alpha)$ divides a binomial and is prime cyclotomic.* But according tot he first Theorem on page 92 this also means that $Nh(\alpha) = p$.

Proof. I will just point out modifications needed, full detail will be on the book. Following what the book does, find a k such that $\alpha \equiv k \mod h(\alpha)$, meaning $k^\lambda \equiv 1 \mod p^n$. Now here comes the catch, unlike what happens in the book $k^\lambda - 1$ need not be $0 \mod p^n$, say it is $p^r \mod p^n$, $r < n$, then Bezout gives us $p^r = a(k^\lambda - 1) + bp^n$ since $Nh(\alpha) = p^n \to h(\alpha)|p^n$ and $1 \equiv \alpha^\lambda \equiv k^\lambda \mod h(\alpha)$ this means that $h(\alpha)|p^r \to Nh(\alpha)|p^{r(\lambda-1)}$ which is not a contradiction.

However, we can still restrict our search for k to those k such that $k^\lambda - 1 \equiv 0 \mod p^n$. We might miss some other k's but that's okay. The next steps would be similar. Again,

assume $p \equiv 1 \mod \lambda$.

Let γ be a primitive root mod p^n (I've proved the existence of primitive roots mod p^n twice before, one for Stein and one for Apostol) then $(\gamma^i)^\lambda \equiv 1 \mod p^n$ if and only if $p^{n-1}(p-1)/\lambda = \mu$ divides i and the solutions are still given by m^j where $m = \gamma^\mu$ and $j = 1, 2, \ldots, \lambda$ just like in the book. This means our $k = m^j$.

We then proceed to the Lemma, here the difference is

$$h(m)h(m^2)\ldots h(m^{\lambda-1}) \equiv 0 \mod p^n$$

i.e. mod p^n instead of mod p. And the more serious difference is that if $h(\alpha)|\alpha - m^j$ then $h(\alpha) \equiv h(m^j) \mod h(\alpha)$ but it doesn't mean that $h(m^j) \equiv 0 \mod p^n$ because it can be that $h(\alpha)|p^r, r < m$ as stated above.

The proof of the lemma is similar

$$\begin{aligned} h(X)h(X^2)\ldots h(X^{\lambda-1}) &= q(X)(X^{\lambda-1} + X^{\lambda-2} + \cdots + 1) + r(X) \\ h(\alpha)h(\alpha^2)\ldots h(\alpha^{\lambda-1}) = p^n &= q(\alpha)(\alpha^{\lambda-1} + \alpha^{\lambda-2} + \cdots + 1) + r(\alpha) \\ \rightarrow p^n &= q(\alpha)\cdot 0 + r(\alpha) \end{aligned}$$

Thus $r(X) = p^n$, the next crucial step is

$$m^{\lambda-1} + m^{\lambda-2} + \cdots + 1 = \frac{m^\lambda - 1}{m-1}$$

again $m^\lambda \equiv 1 \mod p^n$ because $m = \gamma^\mu \not\equiv 1 \mod p^n$ since γ is a primitive root and $p^{n-1}(p-1) = \lambda\mu$ thus there is at least .

For the last step, we need to show that $h(\alpha)$ divides $\alpha - m^j$ by showing that $Nh(\alpha)$ divides $(\alpha - m^j)h(\alpha^2)h(\alpha^3)\ldots h(\alpha^{\lambda-1})$. Again

$$\begin{aligned} h(X) &= q(X)(X - m^j) + r \\ h(m^j) = p^n &= q(m^j)\cdot 0 + r \end{aligned}$$

thus $r \equiv 0 \mod p^n$. Then

$$\begin{aligned} (\alpha - m^j)h(\alpha^2)h(\alpha^3)\ldots h(\alpha^{\lambda-1}) &= (\alpha - m^j)\cdot q(\alpha^2)(\alpha - m^j)q(\alpha^3)(\alpha^3 - m^j)\cdots q(\alpha^{\lambda-1})(\alpha^{\lambda-1} - m^j) \\ &= N(\alpha - m^j)q(\alpha^2)q(\alpha^3)\ldots q(\alpha^{\lambda-1}) \end{aligned}$$

and the key is that

$$N(\alpha - m^j) = \frac{m^{j\lambda} - 1}{m^j - 1}$$

again, since $j = 1, 2, \ldots, \lambda - 1$, $m^j \not\equiv 1 \mod p^n$ and $m^{j\lambda} \equiv \gamma^{j\mu\lambda} \equiv 1 \mod p^n$ thus $N(\alpha - m^j)$ is divisible by $p^n = Nh(\alpha)$ and so $h(\alpha)$ divides $\alpha - m^j$.

Here's why $h(\alpha)$ might not be prime, because we can no longer assume that if $f(\alpha)g(\alpha) \equiv 0 \mod h(\alpha)$ then $f(k)g(k) \equiv 0 \mod p^n$ and vice versa. Even if we can establish that fact $f(k)g(k) \equiv 0 \mod p^n$ still doesn't say that $f(k) \equiv 0 \mod p^n$ or $g(k) \equiv 0 \mod p^n$ it might be that $p^r | f(k)$ and $p^s | g(k)$ with $r + s = n$.

But this situation can be salvaged if $h(\alpha)|p$ because then the arguments in the book all hold, *i.e.* $f(\alpha)g(\alpha) \equiv 0 \mod h(\alpha) \rightarrow f(k)g(k) \equiv 0 \mod p$ because otherwise Bezout tells us that $1 = af(k)g(k) + bp$ is divisible by $h(\alpha)$ implying that $h(\alpha)$ is a unit but $Nh(\alpha) = p^n$. The rest of the proof follows just as what is shown in the book.

Page 94, last statement of proof of Lemma, "because $m^\lambda \equiv 1 \mod p$ and $m \not\equiv 1 \mod p$". Note that $m = \gamma^\mu$ where γ is a primitive root mod p and that $\lambda\mu = p - 1$, thus $m = \gamma^\mu \not\equiv 1$ and of course consequently $m^\lambda = \gamma^{\mu\lambda} = \gamma^{p-1} \equiv 1$.

Page 95, top of page, $N(\alpha - k) = \frac{k^\lambda - 1}{k - 1}$, here $k \not\equiv 1$ because $k = m^j$ where $m = \gamma^\mu$, γ a primitive root and $\mu\lambda = p - 1$ thus $m = \gamma^\mu \not\equiv 1$. But m^j can still be one, however, here $j = 1, 2, \ldots, \lambda - 1$ (λ not included) thus $\gamma^{\mu j} \not\equiv 1$.

Page 95, top paragraph, conclusion of proof of theorem, note that $Nh(\alpha) = p$ thus $h(\alpha)|p$.

Page 95, Problem 1. This is the same as Page 88, Problem 18.

Page 95, Problem 2. This is the same as Page 88, Problem 19.

Page 96, Problem 3. This is an interesting one as we want to show that unique factorization fails because we have irreducibles that are not prime. The only assumption we are allowed to make is that every cyclotomic integer is a product of irreducibles.

First, if $h(\alpha)$ is irreducible (and not a unit since a unit is prime) but not prime then there must be a number it divides that is not itself or a unit multiple of itself. If the only number it divides is just itself or a unit multiple of itself since $h(\alpha)$ is irreducible than it must be prime. Note that only units divide other units.

Therefore there is at least one other number, say $w(\alpha)$, that is divisible by $h(\alpha)$. Our assumption tells us that $w(\alpha)$ is a product of irreducibles therefore we can express

$$w(\alpha) = f_1(\alpha)f_2(\alpha)\dots f_n(\alpha)$$

where $f_i(\alpha)$ are not $h(\alpha)$ or a unit multiple of it otherwise $h(\alpha)$ divides one of the factors of $w(\alpha)$ and it will be prime. This means that

$$w(\alpha) = h(\alpha)y(\alpha) = f(\alpha)f_2(\alpha)\dots f_n(\alpha)$$

and by assumption $y(\alpha)$ is a product of irreducibles and so we have shown that there are at least two ways of factorizing $w(\alpha)$.

Page 96, Problem 4. We are calculating the norm of various binomials, the trick here is to use the hint

$$\begin{aligned}(x+y)N(x+\alpha y) &= (x+y)(x+\alpha y)(x+\alpha^2 y)\dots(x+\alpha^{\lambda-1}y)\\ &= x^\lambda + y^\lambda\end{aligned}$$

which is the identity at the beginning of the Chapter, Page 76. So for $\lambda = 5$

$$\begin{aligned} N(1+\alpha) &= 1 & N(3-2\alpha) &= 211\\ N(2+\alpha) &= 11 & N(4+\alpha) &= 205\\ N(2-\alpha) &= 31 & N(5+2\alpha) &= 451\\ N(3+\alpha) &= 61 & N(5-4\alpha) &= 2101\\ N(3-\alpha) &= 121 & N(7+\alpha) &= 2101\\ N(3+2\alpha) &= 55 \end{aligned}$$

And for $\lambda = 7$

$$\begin{aligned} N(2+\alpha) &= 43 & N(4-\alpha) &= 5461\\ N(2-\alpha) &= 127 & N(4+3\alpha) &= 2653\\ N(3+\alpha) &= 547 & N(4-3\alpha) &= 14197\\ N(3-\alpha) &= 1093 & N(5+\alpha) &= 13021\\ N(3+2\alpha) &= 463 & N(5+2\alpha) &= 11179\\ N(3-2\alpha) &= 2059 & N(5+3\alpha) &= 10039\\ N(4+\alpha) &= 3277 & N(5+4\alpha) &= 10501 \end{aligned}$$

And I calculated all these by hand :)

Page 96, Problem 5. Show that if a prime p divides $N(x+\alpha y)$ then $p \equiv 1 \mod \lambda$ without assuming a prime $h(\alpha)$ divides p. From Problem 4 we know that $N(x+\alpha y) = \frac{x^\lambda + y^\lambda}{x+y}$.

It is actually similar to Page 87, Problem 9, the fact that p divides $N(x+\alpha y)$ means $N(x+\alpha y) \equiv 0 \mod p$. We then factorize

$$N(x+\alpha y) = \frac{x^\lambda + y^\lambda}{x+y} = (y^{\lambda-1} - xy^{\lambda-2} + \cdots + x^{\lambda-1})$$
$$\rightarrow (y^{\lambda-1} - xy^{\lambda-2} + \cdots + x^{\lambda-1}) \equiv 0 \mod p$$

since x and y are co-prime p doesn't divide any of them. Do the same trick as Page 87 Problem 9 to massage the equivalence relation into

$$k^{\lambda-1} - k^{\lambda-2} + \cdots + 1 \equiv 0 \mod p$$

where $k \equiv x^{-1}y$ or $y^{-1}x$, see Problem 9 Page 87 for details. We now do the trick we always do when dealing with a geometric series. Multiply the whole thing by k and then add them up

$$k \times (1 - k + k^2 - \cdots + k^{\lambda-1}) \equiv k - k^2 + k^3 - \cdots + k^\lambda \equiv 0 \mod p$$
$$\rightarrow (1+k) \times (1 - k + k^2 - \cdots + k^{\lambda-1}) \equiv 1 + k^\lambda \equiv 0 \mod p$$

since λ is odd it's either $k \equiv -1$ or $k^\lambda \equiv -1 \mod p$. But if $k \equiv -1$ then we have

$$1 - k + k^2 - \cdots + k^{\lambda-1} = 1 + 1 + 1 + \cdots + 1 \equiv 0 \mod p$$
$$\rightarrow \lambda \equiv 0 \mod p$$

but since both λ and p are both prime the only possibility is that $p = \lambda$ and in that case $p \equiv 0 \mod \lambda$ which is the first result we need.

If $k^\lambda \equiv -1 \mod p$ then $k^{2\lambda} \equiv 1 \mod p$. Since 2 and λ are prime, the order (or exponent) of k must be either 2, λor 2λ and each must divide $p-1$ according to Fermat's Little Theorem. for the cases of the order being λ or 2λ this means that $\lambda | p-1$ or $2\lambda | p-1$, either way this means that $p - 1 \equiv 0 \mod \lambda$.

If the order of k is 2 then k can only be $+1$ or -1 (as $x^2 \equiv 1$ can only have two solutions). But $k \equiv -1$ is already covered above resulting in $p \equiv 0 \mod \lambda$ and as shown above $1 + k^\lambda \equiv 0 \mod p$ which means that k cannot be 1.

Page 96, Problem 6. We are now asked to find the prime factors of the norms we found in Problem 4 using information from Problem 5. for $\lambda = 5$

$$\begin{aligned}
N(1+\alpha) &= 1 = 1\cdot 1 & N(3-2\alpha) &= 211 = 211\cdot 1\\
N(2+\alpha) &= 11 = 11\cdot 1 & N(4+\alpha) &= 205 = 41\cdot 5\\
N(2-\alpha) &= 31 = 31\cdot 1 & N(5+2\alpha) &= 451 = 41\cdot 41\\
N(3+\alpha) &= 61 = 61\cdot 1 & N(5-4\alpha) &= 2101 = 191\cdot 11\\
N(3-\alpha) &= 121 = 11\cdot 11 & N(7+\alpha) &= 2101 = 191\cdot 11\\
N(3+2\alpha) &= 55 = 11\cdot 5
\end{aligned}$$

For the bigger numbers, since they are odd, it cannot be a multiple of $5(2n+1)+1$ so it can only be a multiple of $11, 21, 31, \ldots$. And the primes in this list are $11, 31, 41, 61, \ldots$ but we need not consider more than these since to do factorization we only need to go to $\sqrt{n}$ and $61^2 = 3721$ already. So we just need if any of these four primes divide the norm, if they don't then the norm is also a prime because any prime divisor of the norm must be one of these four from Problem 5.

And for $\lambda = 7$

$$\begin{aligned}
N(2+\alpha) &= 43 = 43\cdot 1 & N(4-\alpha) &= 5461 = 127\cdot 43\\
N(2-\alpha) &= 127 = 127\cdot 1 & N(4+3\alpha) &= 2653 = 379\cdot 7\\
N(3+\alpha) &= 547 = 547\cdot 1 & N(4-3\alpha) &= 14197 = 14197\cdot 1\\
N(3-\alpha) &= 1093 = 1093\cdot 1 & N(5+\alpha) &= 13021 = 449\cdot 29\\
N(3+2\alpha) &= 463 = 463\cdot 1 & N(5+2\alpha) &= 11179 = 1597\cdot 7\\
N(3-2\alpha) &= 2059 = 71\cdot 29 & N(5+3\alpha) &= 10039 = 10039\cdot 1\\
N(4+\alpha) &= 3277 = 113\cdot 29 & N(5+4\alpha) &= 10501 = 10501\cdot 1
\end{aligned}$$

Again, all these are odd, so the only possible factors are of the form $7(2n) + 1 = 15, 29, 43, 57, 71, 85, 99, 113, 127$, again we only need to go up to $\sqrt{n}$ and here $n \sim 10000 \to \sqrt{n} \sim 100$, the only primes in that list are $29, 43, 71, 113, 127$.

I initially thought that this was just a calculation but it also betrays the fact that Problem 5 simplifies the factorization considerably as explained above. I did everything

by hand and the only mistake I made was 2653 because I didn't check that it was a multiple of 7.

Page 96, Problem 7. Here we are again calculating norms, $N(9-\alpha)$ with $\lambda = 5$, directly and using the fact that it is $N(9-\alpha) = N(3-\alpha)N(3+\alpha)$ because

$$N(9-\alpha) = N(9-\alpha^2) = N\{(3-\alpha)(3+\alpha)\} = N(3-\alpha)N(3+\alpha)$$

A direct calculation gives you $N(9-\alpha) = \frac{9^5-1^5}{8} = 7381$, again by hand. We have calculated $N(3-\alpha)$ and $N(3+\alpha)$ in Problem 4 and their product is $61 \cdot 121 = 7381$, again by hand.

Page 96, Problem 8. Prove that for $p \equiv 1 \mod \lambda$ the prime factorization of p is unique. If $h_1(\alpha)$ and $h_2(\alpha)$ are both factors of p then they are unit multiples of one another's conjugate.

What we know is that since $h_{1,2}|p \to Nh_{1,2}(\alpha)|p^{\lambda-1}$. Note that $Np = p^{\lambda-1}$ and not p. This means that

$$Nh_1(\alpha) = p^j$$
$$Nh_2(\alpha) = p^k$$

where $j, k = 1, 2, \ldots, \lambda - 1$ because $Nh_{1,2}(\alpha)$ is an integer. If $Nh_1(\alpha) = Nh_2(\alpha)$ then we are done, we just need to follow the same steps as the proof of the Third Corollary on Page 95.

But it's not easy to show that the norms are equal. Another way is to find a binomial whose norm is a multiple of p given such prime p. Since if $p|N(x+\alpha^j y)$ and $h_{1,2}(\alpha)|p$ then we have $h_{1,2}(\alpha)$ being a prime divide one of the factors of $N(x+\alpha^j y)$ which means that $h_{1,2}(\alpha)$ divides a conjugate of the binomial which is also a binomial. The First Theorem on Page 92 says that if a prime $h(\alpha)$ divides a binomial then its norm is prime and since $Nh_{1,2}(\alpha)|p^{\lambda-1}$ we have $Nh_{1,2}(\alpha) = p$ and from the Third Corollary on Page 93 we have $h_2(\alpha)$ is a unit times a conjugate of $h_1(\alpha)$.

So the task now is to show that we can find a binomial whose norm is divisible by p. From Problem 4 we know that the norm of a binomial is given by $\frac{x^\lambda+y^\lambda}{x+y}$ and we want this

thing to be $\equiv 0 \mod p$. So we don't want $x + y$ to be $0 \mod p$ obviously. Thus

$$\begin{aligned} x^\lambda + y^\lambda &\equiv 0 \mod p \\ x^\lambda &\equiv -y^\lambda \mod p \\ \left(\frac{x}{-y}\right)^\lambda &\equiv 1 \mod p \end{aligned}$$

Since p is prime we have primitive roots $\gamma \mod p$. And Fermat's Little Theorem gives us $\gamma^{p-1} \equiv 1 \mod p$ but here $p \equiv 1 \mod \lambda \to p - 1 = \mu\lambda$. Thus we can assign

$$\begin{aligned} \gamma^\mu &\equiv \frac{x}{-y} \mod p \\ \to (-y)\gamma^\mu &\equiv x \mod p \end{aligned}$$

Thus we can choose any $y \not\equiv 0 \mod p$ we want, multiply it with $-\gamma^\mu$ to get our x, the only condition is that $x + y \not\equiv 0 \mod p$ but this is guaranteed because

$$x + y \equiv y(1 - \gamma^\mu) \mod p$$

and γ being a primitive root and $\mu\lambda = p - 1$ means that $\gamma^\mu \not\equiv 1 \mod p$ and $x + \alpha y$ will be our binomial. As a aside, this shows that if $h(\alpha)|p$ and $p \equiv 1 \mod \lambda$ then $Nh(\alpha) = p$.

Page 96, Problem 9. Filling in the details of Kummer's proof that if $Nh(\alpha)$ is prime then $\alpha \equiv k \mod h(\alpha)$.

First step, let $h(\alpha^2)h(\alpha^3)\dots h(\alpha^{\lambda-1}) = H(\alpha) = A_0 + A_1\alpha + A_2\alpha^2 + \cdots + A_{\lambda-1}\alpha^{\lambda-1}$. We then create the following somewhat curious object $\alpha^{-n}H(\alpha) + \alpha^{-2n}H(\alpha^2) + \cdots + \alpha^{-(\lambda-1)n}H(\alpha^{\lambda-1})$.

One thing to note here is, since we are working with negative powers of α,

$$\begin{aligned} 1 + \alpha + \cdots + \alpha^{\lambda-1} &= 0 \\ \to \alpha^{-(\lambda-1)} \times (1 + \alpha + \cdots + \alpha^{\lambda-1}) &= 0 \\ \to \alpha^{-(\lambda-1)} + \alpha^{-(\lambda-2)} + \cdots + 1 &= 0 \end{aligned}$$

which is just a (negative) conjugate of $1 + \alpha + \cdots + \alpha^{\lambda-1}$, again this is guaranteed by the fact that any integer multiple of the unit group $(\mathbb{Z}/\lambda\mathbb{Z})^*$ is also the unit group itself as long as the multiplier is not a multiple of λ.

To calculate the curious object, let's examine it term by term, let's take $A_i\alpha^i$ of $H(\alpha)$ then

$$\begin{aligned} A_i\alpha^i &\to A_i(\alpha^{i-n} + \alpha^2 i - n + \cdots + \alpha^{(\lambda-1)(i-n)}) \\ &= A_i\{(\alpha^{i-n})^1 + (\alpha^{i-n})^2 + \cdots + (\alpha^{i-n})^{\lambda-1}\} = A_i(-1) \end{aligned}$$

which is just A_i multiplied by a (maybe negative) conjugate of $\alpha + \cdots + \alpha^{\lambda-1}$, note that hte constant 1 is missing, therefore the terms in curly braces add up to -1. The above is true only when $i - n \neq 0$ if $i = n$ then we get $A_i(\lambda - 1)$ thus

$$\alpha^{-n}H(\alpha) + \alpha^{-2n}H(\alpha^2) + \cdots + \alpha^{-(\lambda-1)n}H(\alpha^{\lambda-1}) = A_n\lambda - (A_0 + A_1 + \cdots + A_{\lambda-1})$$

The next curious object is $\alpha^{-n}(1-\alpha)H(\alpha) + \alpha^{-2n}(1-\alpha^2)H(\alpha^2) + \cdots + \alpha^{-(\lambda-1)n}(1-\alpha^{\lambda-1})H(\alpha^{\lambda-1})$, again, take one term $A_i\alpha^i$ from $H(\alpha)$ and examine what happens to this term

$$\begin{aligned} A_i\alpha^i &\to A_i\{(1-\alpha)(\alpha^{i-n}) + (1-\alpha^2)(\alpha^{i-n})^2 + \cdots + (1-\alpha^{\lambda-1})(\alpha^{i-n})^{\lambda-1}\} \\ &= A_i\{(\alpha^{i-n}) + (\alpha^{i-n})^2 + \cdots + (\alpha^{i-n})^{\lambda-1} - (\alpha^{i-n+1}) - (\alpha^{i-n+1})^2 - \cdots - (\alpha^{i-n+1})^{\lambda-1}\} \\ &= A_i\{-1 - (-1)\} \\ &= 0 \end{aligned}$$

the only exception to the above rule is when $i = n \to A_i(\lambda - 1 - (-1)) = A_i\lambda$ and $i = n - 1 \to A_i(-1 - \lambda + 1) = -A_i\lambda$ thus

$$\alpha^{-n}(1-\alpha)H(\alpha) + \alpha^{-2n}(1-\alpha^2)H(\alpha^2) + \cdots + \alpha^{-(\lambda-1)n}(1-\alpha^{\lambda-1})H(\alpha^{\lambda-1}) = \lambda(A_n - A_{n-1})$$

The next thing we need to show is that $H(\alpha^j)H(\alpha^k) \equiv 0 \mod p$. Note that $Nh(\alpha) = p$ and $H(\alpha) = h(\alpha^2)h(\alpha^3)\ldots h(\alpha^{\lambda-1})$ thus

$$H(\alpha^j)H(\alpha^k) = \{h(\alpha^{2j})h(\alpha^{3j})\ldots h(\alpha^{(\lambda-1)j})\} \cdot \{h(\alpha^{2k})h(\alpha^{3k})\ldots h(\alpha^{(\lambda-1)k})\}$$

if $j \not\equiv k \mod p$ then there's an $i \not\equiv 1, 0 \mod p$ such that $ji \equiv k \mod p$ thus

$$\begin{aligned} H(\alpha^j)H(\alpha^k) &= \{h(\alpha^{2j})h(\alpha^{3j})\ldots h(\alpha^{(i-1)j})h(\alpha^{(i+1)j})\ldots h(\alpha^{(\lambda-1)j})\} \times \\ &\quad \{h(\alpha^{ij=k})h(\alpha^{2k})h(\alpha^{3k})\ldots h(\alpha^{(\lambda-1)k})\} \\ &= \{h(\alpha^{2j})h(\alpha^{3j})\ldots h(\alpha^{(i-1)j})h(\alpha^{(i+1)j})\ldots Nh(\alpha) \end{aligned}$$

and since $Nh(\alpha) = p$ the whole thing is $0 \mod p$. To simplify things let's denote

$$\begin{aligned} F(n) &= \alpha^{-n}(1-\alpha)H(\alpha) + \alpha^{-2n}(1-\alpha^2)H(\alpha^2) + \cdots + \alpha^{-(\lambda-1)n}(1-\alpha^{\lambda-1})H(\alpha^{\lambda-1}) \\ &= \lambda(A_n - A_{n-1}) \end{aligned}$$

One important thing to note is that n is not bounded, since $\alpha^\lambda = 1$ we can have n to take any value, for example $A_{-5} = A_{\lambda-5 \mod \lambda}$. Therefore since the cross terms $H(\alpha^j)H(\alpha^k) \equiv 0$ for $j \not\equiv k$ we have

$$\begin{aligned} F^2(n) &\equiv \alpha^{-2n}(1-\alpha)^2H^2(\alpha) + \alpha^{-4n}(1-\alpha^2)^2H^2(\alpha^2) + \cdots + \\ &\qquad \alpha^{-2(\lambda-1)n}(1-\alpha^{\lambda-1})^2H^2(\alpha^{\lambda-1}) \\ F(n+1)F(n-1) &\equiv \alpha^{-2n}(1-\alpha)^2H^2(\alpha) + \alpha^{-4n}(1-\alpha^2)^2H^2(\alpha^2) + \cdots + \\ &\qquad \alpha^{-2(\lambda-1)n}(1-\alpha^{\lambda-1})^2H^2(\alpha^{\lambda-1}) \end{aligned}$$

Thus

$$\begin{aligned} F^2(n) - F(n+1)F(n-1) \equiv 0 \equiv \lambda^2(A_n - A_{n-1})^2 - \lambda^2(A_{n+1} - A_n)(A_{n-1} - A_{n-2}) \mod p \\ \rightarrow \frac{(A_n - A_{n-1})}{(A_{n+1} - A_n)} \equiv \frac{(A_{n-1} - A_{n-2})}{(A_n - A_{n-1})} \mod p \end{aligned}$$

But the above relationship is true for any n since it is just the identity $F^2(n) - F(n+1)F(n-1) \equiv 0$, thus if we denote $\xi \equiv \frac{(A_n - A_{n-1})}{(A_{n+1} - A_n)}$, ξ must be independent of n. To see this, start with $F^2(2) - F(3)F(1) \equiv 0$ to get

$$\frac{(A_2 - A_1)}{(A_3 - A_2)} \equiv \frac{(A_1 - A_0)}{(A_2 - A_1)} \mod p$$

next, set $n = 3, F^2(3) - F(4)F(2) \equiv 0$ to get

$$\frac{(A_3 - A_2)}{(A_4 - A_3)} \equiv \frac{(A_2 - A_1)}{(A_3 - A_2)} \mod p$$

but $\frac{(A_2 - A_1)}{(A_3 - A_2)} \equiv \frac{(A_1 - A_0)}{(A_2 - A_1)}$ incrementing n we will get the ratio for the next n and therefore all the ratios are the same which means that $\xi \equiv \frac{(A_n - A_{n-1})}{(A_{n+1} - A_n)}$ is independent of n.

The only potential problem would be when some of the differences $A_l - A_{l-1}$ are zero. But as mentioned before n can have any value due to $\alpha^\lambda = 1$ thus we can for example set $F^2(-1) \equiv \lambda^2(A_{-1 \equiv \lambda-1 \mod \lambda} - A_{-2 \equiv \lambda-2 \mod \lambda})^2$, therefore if any of the differences is zero then all of them will be zero which means that $A_0 = A_1 = A_2 = \cdots = A_{\lambda-1}$ therefore

$H(\alpha) = A_0(1 + \alpha + \cdots + \alpha^{\lambda-1}) = 0$. This cannot be because $Nh(\alpha) = p \neq 0$ and $Nh(\alpha) = h(\alpha)H(\alpha)$ therefore ξ is well defined.

Now, if we rewrite the identity

$$\begin{aligned}\frac{(A_n - A_{n-1})}{(A_{n+1} - A_n)} \equiv \frac{(A_{n-1} - A_{n-2})}{(A_n - A_{n-1})} &\to (A_n - A_{n-1}) \equiv (A_{n+1} - A_n)\frac{(A_{n-1} - A_{n-2})}{(A_n - A_{n-1})} \\ &\to (A_n - A_{n-1}) \equiv (A_{n+1} - A_n)\xi \\ &\to \xi A_n - A_{n-1} \equiv \xi A_{n+1} - A_n\end{aligned}$$

Again, just like before, this means that $\xi A_m - A_{m-1}$ is constant regardless what m is. The last step is show that $(\alpha - \xi)H(\alpha) \equiv 0 \mod p$

$$\begin{aligned}(\alpha - \xi)H(\alpha) &\equiv (A_0\alpha + A_1\alpha^2 + \cdots + A_{\lambda-1}\alpha^{\lambda}) - (\xi A_0 + \xi A_1\alpha + \cdots + \xi A_{\lambda-1}\alpha^{\lambda-1}) \\ &\equiv (A_0 - \xi A_1)\alpha + (A_1 - \xi A_2)\alpha^2 + \cdots + (A_{\lambda-2} - \xi A_{\lambda-1})\alpha^{\lambda-1} + (A_{\lambda-1} - \xi A_0) \\ &\equiv (A_0 - \xi A_1)(\alpha + \alpha^2 + \cdots + \alpha^{\lambda-1} + 1) \\ &\equiv 0\end{aligned}$$

because the terms in brackets is the usual zero. Thus $(\alpha - \xi)H(\alpha) \equiv 0 \mod p$ and using the usual trick

$$h(\alpha)g(\alpha) = f(\alpha) \iff Nh(\alpha)g(\alpha) = f(\alpha)h(\alpha^2)h(\alpha^3)\ldots h(\alpha^{\lambda-1})$$

we have here

$$h(\alpha)g(\alpha) = (\alpha - \xi) \iff Nh(\alpha)g(\alpha) = (\alpha - \xi)h(\alpha^2)h(\alpha^3)\ldots h(\alpha^{\lambda-1}) = (\alpha - \xi)H(\alpha)$$

which means $h(\alpha)|(\alpha - \xi)$

Page 96, Problem 10. We need to use the theorems in Section 4.3 to prove that if a prime $p \equiv 1 \mod \lambda$ is divisible by prime $h(\alpha)$ then there are precisely $\lambda - 1$ solutions to $k^{\lambda} \equiv 1 \mod \lambda$ with $k \not\equiv 1 \mod \lambda$.

Just like Problem 8, $h(\alpha)|p$ means $Nh(\alpha)|p^{\lambda-1}$, to use the theorems we have to either show that $Nh(\alpha) = p$ or $h(\alpha)$ divides a binomial. But Problem 8 already tells us that $Nh(\alpha) = p$ which means that according to the second Theorem on Page 92 $h(\alpha)$ divides a binomial.

Since $h(\alpha)$ divides a binomial $x+\alpha^j y$ and a prime p from the Theorem on Page 91 we have $f(\alpha) \equiv g(\alpha) \mod h(\alpha) \iff f(k) \equiv g(k) \mod p$. From page 92 we know that

$$\alpha^{\lambda-1} + \alpha^{\lambda-2} + \cdots + \alpha + 1 \equiv 0 \mod h(\alpha) \iff k^{\lambda-1} + k^{\lambda-2} + \cdots + k + 1 \equiv 0 \mod p$$

which also means that $k^\lambda - 1 = (k-1)(k^{\lambda-1} + k^{\lambda-2} + \cdots + k + 1) \equiv 0 \mod p$. So it is obvious that $k \equiv 1$ is a solution to $k^\lambda - 1$, the other solutions we can get from the fact that the conjugates of $\alpha^{\lambda-1} + \alpha^{\lambda-2} + \cdots + \alpha + 1$ is just itself

$$0 = \alpha^{\lambda-1} + \alpha^{\lambda-2} + \cdots + \alpha + 1 = (\alpha^j)^{\lambda-1} + (\alpha^j)^{\lambda-2} + \cdots + (\alpha^j) + 1$$

Theorem on Page 91 gives us $f(\alpha) \equiv g(\alpha) \mod h(\alpha) \iff f(k) \equiv g(k) \mod p$ then

$$(\alpha^j)^{\lambda-1} + (\alpha^j)^{\lambda-2} + \cdots + (\alpha^j) + 1 \equiv 0 \iff (k^j)^{\lambda-1} + (k^j)^{\lambda-2} + \cdots + (k^j) + 1 \equiv 0 \mod p$$

since j runs from $1, 2, \ldots, \lambda-1$ these k^j give us the other $\lambda-1$ solution to $k^\lambda \equiv 1 \mod \lambda$.

The next part of the question asks us to prove this again but this time without using the fact that $h(\alpha)$ is prime. This is actually quite straightforward, it's even given in Stein's ent.pdf. From $p \equiv 1 \mod \lambda$ we have $p - 1 = \mu\lambda$ therefore

$$k^{p-1} - 1 = k^{\mu\lambda} - 1 = (k^\lambda - 1)((k^\lambda)^{\mu-1} + (k^\lambda)^{\mu-2} + \cdots + (k^\lambda) + 1)$$

The second bracket is a polynomial of degree $\lambda\mu - \lambda$ so it at most has $\lambda\mu - \lambda$ roots the first bracket is a polynomial of degree λ so it at most has λ roots, the LHS however is $k^{p-1} - 1$ and every remainder of p is a root and there are $p - 1 = \mu\lambda$ roots, thus each bracket in the RHS must have the maximum number of roots and $k^\lambda - 1$ must have exactly λ roots.

Page 96, Problem 11. Here we have $\lambda = 5$, $f(\alpha) = g(\alpha)$ and we want to find which prime p gives us $f(7) \equiv g(7) \mod p$.

According to Theorem on Page 91, this means that $k = 7$ where $\alpha \equiv k \mod h(\alpha)$. The simplest guess for $h(\alpha)$ is $\alpha - 7$. If $N(\alpha - 7)$ is prime then from Page 92 Theorems we have $\alpha - 7$ to be prime and since it divides itself we have $\alpha \equiv 7 \mod \alpha - 7$. And $N(\alpha - 7)$ is the prime p we need.

So let's calculate $N(\alpha - 7) = \frac{7^5 - 1^5}{6} = 2801$ and lucky for us it is prime, thus $p = 2801$.

Page 96, Problem 12. Prove that $f(\alpha) = g(\alpha)$ if and only if $f(X) - g(X) = q(X)(X^{\lambda-1} + X^{\lambda-2} + \cdots + 1)$. Conclude that if $k^{\lambda-1} + k^{\lambda-2} + \cdots + 1 \equiv 0 \mod p$ then $f(\alpha) = g(\alpha)$ implies $f(k) \equiv g(k) \mod p$.

The if only if is easy in the only if direction. If $f(X) - g(X) = q(X)(X^{\lambda-1} + X^{\lambda-2} + \cdots + 1)$ then setting $X = \alpha$ we get $f(\alpha) - g(\alpha) = q(\alpha)(\alpha^{\lambda-1} + \alpha^{\lambda-2} + \cdots + 1) = q(\alpha) \cdot 0 = 0$. The other direction is not too difficult either, assume $f(X) - g(X)$ is some polynomial in X. We now want to use the division algorithm on this with $h(X) = X^{\lambda-1} + X^{\lambda-2} + \cdots + 1$ as the divisor, we then get

$$f(X) - g(X) = Q(X)(X^{\lambda-1} + X^{\lambda-2} + \cdots + 1) + r(X)$$

with $r(X)$ having a lesser degree than that of $h(X)$. If we set $X = \alpha$ we get (knowing that $f(\alpha) = g(\alpha) \to 0 = f(\alpha) - g(\alpha)$)

$$\begin{aligned} 0 = f(\alpha) - g(\alpha) &= Q(\alpha)(\alpha^{\lambda-1} + \alpha^{\lambda-2} + \cdots + 1) + r(\alpha) \\ 0 &= Q(\alpha) \cdot 0 + r(\alpha) \\ \to 0 &= r(\alpha) \end{aligned}$$

and from Page 88, Problem 15, we know that $r(\alpha) = c(\alpha^{\lambda-1} + \alpha^{\lambda-2} + \cdots + 1)$ which means that

$$\begin{aligned} f(X) - g(X) &= Q(X)(X^{\lambda-1} + X^{\lambda-2} + \cdots + 1) + c(X^{\lambda-1} + X^{\lambda-2} + \cdots + 1) \\ &= (Q(X) + c)(X^{\lambda-1} + X^{\lambda-2} + \cdots + 1) \\ &= q(X)(X^{\lambda-1} + X^{\lambda-2} + \cdots + 1) \end{aligned}$$

Now the next part of the question, it is straightforward enough, we already have $f(\alpha) = g(\alpha) \iff f(X) - g(X) = q(X)(X^{\lambda-1} + X^{\lambda-2} + \cdots + 1)$, we now set $X = k$ to get $f(k) - g(k) = q(k)(k^{\lambda-1} + k^{\lambda-2} + \cdots + 1) \equiv 0 \mod p \to f(k) \equiv g(k) \mod p$ since the problem tells us that $k^{\lambda-1} + k^{\lambda-2} + \cdots + 1 \equiv 0 \mod p$.

Page 97. Bottom. $\alpha + 2$ is prime because $N(\alpha + 2) = 11$ is prime which satisfies the condition of Theorem on page 92. The next statement $g(\alpha)$ is divisible by $\alpha + 2$ if and only if $g(-2) \equiv 0 \mod 11$. This comes from Theorem of Page 91, $f(\alpha) \equiv g(\alpha) \mod h(\alpha) \iff f(k) \equiv g(k) \mod p$.

From Theorem on Page 92, since $N(\alpha + 2) = 11$ is prime $\alpha + 2$ is a cyclotomic prime and it divides a binomial, here the prime is $h(\alpha) = \alpha + 2$ and the binomial is also $\alpha + 2$. And since $\alpha + 2 \equiv 0 \mod h(\alpha)$, a trivial identity, we therefore have $\alpha \equiv -2 \mod h(\alpha)$,

$k = -2$ and $p = Nh(\alpha) = 11$ therefore Theorem on Page 91 gives us

$$g(\alpha) \equiv (\alpha + 2)y(\alpha) \mod h(\alpha) \Longleftrightarrow g(-2) \equiv (-2 + 2)y(-2) \equiv 0 \mod 11$$

Page 98. First line, "product of 4 distinct prime factors each of norm 11". Note that the norm of an ordinary integer i is $i^{\lambda-1}$ and **not** i. This is because $N(i) = (i)(i)(i)\ldots(i) = i^{\lambda-1}$.

Page 98. Top page, "The only factors of norm $5(= \lambda)$ are units time $\alpha - 1$." How to see this? Assume otherwise, but we know that $N(\alpha - 1) = \lambda$. If there are other prime factors say $f(\alpha)$ then it must be that

$$\begin{aligned} \lambda = f(\alpha)g(\alpha) = N(\alpha - 1) = (\alpha - 1)^{\lambda-1}u(\alpha) \\ \rightarrow f(\alpha) \mid (\alpha - 1) \end{aligned}$$

the RHS of the first line is due to the fact that any conjugate $\alpha^j - 1$ is a unit multiple of $\alpha - 1$. Since $f(\alpha)|(\alpha - 1)$ it means that $Nf(\alpha)|N(\alpha - 1) \rightarrow Nf(\alpha)|\lambda$ which means that the quotient of $(\alpha - 1)/f(\alpha)$ is a unit, hence $f(\alpha) = (\alpha - 1)u(\alpha)$ thus the only prime factors of λ is $(\alpha - 1)$.

Page 98. Lower half dividing one cyclotomic with another, here we divide $4\alpha^2 - 5$ by $\alpha + 2$, we can still use the normal notation like $(\alpha + 2)^{-1}$ just need to keep track what it means.

Page 99. Last paragraph, just a short comment, note that the cyclotomic integers do not form a group under multiplication because there's obviously no inverse for non-units, they do form a group under addition. Therefore, $\alpha^4 \equiv k^4 \mod h(\alpha)$ doesn't mean that $\alpha \equiv k$ because otherwise in the example of normal integers we can multiply both sides with the inverse $1 \equiv (\alpha^{-1}k)^4$, one of the roots is obviously 1 and we can infer $\alpha^{-1}k \equiv 1 \rightarrow \alpha \equiv k$ but if $\alpha \equiv k$ we certainly have $\alpha^4 \equiv k^4$.

Page 99. Last paragraph, "$a^4 \not\equiv 1 \mod 29$", the reason we don't include $a^4 \equiv 1$ is because then $\alpha \equiv 1 \mod h(\alpha) \rightarrow h(\alpha)|(\alpha - 1) \rightarrow Nh(\alpha)|N(\alpha - 1) = \lambda$, but here we want $Nh(\alpha) = 29$ or more generally $Nh(\alpha) = p \equiv 1 \mod \lambda$.

Page 100. Top page, we started the guess of $g(-13) \equiv 0 \mod 29$ with $g(\alpha) \equiv \alpha^2 - \alpha^4 + 1$ why not start with $g(\alpha) \equiv \alpha + 13$ since this is the simplest guess? One reason I

can think of is that he already knew :) problem is that $N(\alpha+13) = 4482037 = 7 \cdot 29 \cdot 22079$. He wanted a simpler example.

Page 100. Mid(ish) page, dividing $\alpha + 4$ by a factor of 29 and $k + 4 \equiv 0 \mod 29$, there's a simple typo, "The solution is $k = 4$", it should've been $k = -4$. Also, even though we are trying to get the factors of $\alpha + 4$ we first try to find a conjugate that is divisible by $-\alpha^4 + \alpha^2 + 1$. Since $(-13)^4 \equiv -4 \mod 29$ we can therefore conclude that $\alpha^4 + 4 \equiv 0$. Once we get all the factors of $\alpha^4 + 4$ we can do a conjugation at the end to get the factors of $\alpha + 4$ by taking $\alpha \to \alpha^2$.

Page 100. Mid page, "$k \equiv k^8 \equiv 16$", note that if $\alpha \equiv k$ then $1 \equiv \alpha^7 \equiv k^7$. Therefore $k^8 \equiv k$.

Page 100. Footnote, last section of footnote, note that $\theta_0 + \theta_1 = -1$.

Page 101. Mid(ish) page, "$N(\alpha-4) \equiv 0 \mod 47$". This is because $N(\alpha-4) = \frac{1^{23}-4^{23}}{1-4}$ but $4^{23} = 2^{2 \cdot 23} \equiv 2^{47-1} \equiv 1 \mod 47$.

Page 106, Problem 1 (a). The key to these problems is to not blindly compute things :) We know from this section that

$$N(\alpha + 2) = (\alpha + 2)(\alpha^2 + 2)(\alpha^3 + 2)(\alpha^4 + 2) = 11$$

Now, instead of massaging the LHS we massage the RHS. The only factor missing from the LHS compared to $N(\alpha + 2)$ is $(\alpha^2 + 2)$ therefore if we multiply $(\alpha^2 + 2)(\alpha^4 + \alpha^3 + 2)$ we should get $(3 - \alpha)$

$$\begin{aligned}(\alpha^2 + 2)(\alpha^4 + \alpha^3 + 2) &= \alpha^6 + \alpha^5 + 2\alpha^2 + 2\alpha^4 + 2\alpha^3 + 4 \\ &= \alpha + 1 + 2\alpha^2 + 2\alpha^4 + 2\alpha^3 + 4 \\ &= -3 + \alpha\end{aligned}$$

Page 106, Problem 1 (b). We know that $N(3 - \alpha) = N(\alpha - 3) = 11^2 = \{(\alpha + 2)(\alpha^2 + 2)(\alpha^3 + 2)(\alpha^4 + 2)\}^2$ since $N(\alpha + 2) = 11$ thus

$$(3 - \alpha)(3 - \alpha^2)(3 - \alpha^3)(3 - \alpha^4) = \{(\alpha + 2)(\alpha^2 + 2)(\alpha^3 + 2)(\alpha^4 + 2)\}^2$$

and we also know that $(\alpha^2 + 2)$ is prime since $N(\alpha^2 + 2) = 11$ a prime. Now we want to

know which conjugate of $3-\alpha$ is divisible by (α^2+2). From

$$\begin{aligned}\alpha^2 &\equiv -2 \mod \alpha^2+2\\ \rightarrow k^2 &\equiv -2 \mod 11\end{aligned}$$

and the fact that $1 \equiv \alpha^{\lambda=5} \equiv k^5 \rightarrow k^6 \equiv k$ we know that $k^6 \equiv (-2)^3 \equiv 3 \mod 11$. So $\alpha \equiv 3 \mod \alpha^2+2$ therefore it is $3-\alpha$ itself that is divisible by α^2+2. But substituting $\alpha \rightarrow 3$ in the other conjugates $3-\alpha^j$ doesn't product $0 \mod 11$ and there are two counts of α^2+2 in the RHS above, therefore both α^2+2 must divide $3-\alpha$, *i.e.* $(\alpha^2+2)^2|(3-\alpha)$.

The quotient is of course a unit since $N(3-\alpha) = N(\alpha^2+2)^2$, now we need to find the unit, we can use the normal algorithm $f(\alpha)g(\alpha) = h(\alpha) \rightarrow g(\alpha) = \frac{h(\alpha)f(\alpha^2)f(\alpha^3)\ldots f(\alpha^{\lambda-1})}{Nf(\alpha)}$, here $h(\alpha) = 3-\alpha$, $f(\alpha) = (\alpha^2+2)^2$ and $Nf(\alpha) = 11^2$ and so

$$g(\alpha) = \frac{(3-\alpha)\{(\alpha+2)(\alpha^3+2)(\alpha^4+2)\}^2}{11^2}$$

But form Problem 1 (a) we know that $(3-\alpha)(\alpha+2)(\alpha^3+2)(\alpha^4+2) = 11(\alpha^4+\alpha^3+4)$ so

$$\begin{aligned}\frac{(3-\alpha)\{(\alpha+2)(\alpha^3+2)(\alpha^4+2)\}^2}{11^2} &= \frac{\cancel{11}(\alpha^4+\alpha^3+4)(\alpha+2)(\alpha^3+2)(\alpha^4+2)}{\cancel{11^2}}\\ &= \frac{(\alpha^4+\alpha^3+4)(\alpha+2)(\alpha^3+2)(\alpha^4+2)}{(\alpha+2)(\alpha^2+2)(\alpha^3+2)(\alpha^4+2)}\\ &= \frac{(\alpha^4+\alpha^3+4)}{(\alpha^2+2)}\end{aligned}$$

to get to the last line I substituted $11 = N(\alpha^2+2)$. Doing the long division we get

$$\frac{(\alpha^4+\alpha^3+4)}{(\alpha^2+2)} = \alpha^2+\alpha-2+2\frac{(3-\alpha)}{(\alpha^2+2)}$$

The last fraction can be done using the usual division algorithm

$$\begin{aligned}\frac{(3-\alpha)}{(\alpha^2+2)} &= \frac{(3-\alpha)(\alpha+2)(\alpha^3+2)(\alpha^4+2)}{11}\\ &= \alpha^4+\alpha^3+2\end{aligned}$$

Therefore

$$\begin{aligned}\frac{(\alpha^4+\alpha^3+4)}{(\alpha^2+2)} &= -\alpha-\alpha^2\\ &= -\alpha(\alpha+1)\end{aligned}$$

$-\alpha$ is obviously a unit $N(\alpha+1)=\frac{1^\lambda+1^\lambda}{1+1}=1$ also a unit, the inverse of this unit is just the product of all of its conjugates (since $Nu(\alpha)=1$).

Page 106, Problem 1 (c). We know from the Section that $N(5+2\alpha)=11\cdot 41$, also $N(\alpha^2+2)=11$ and $N(3\alpha^4+3\alpha^2+1)=41$ from Page 98.

Also from Page 98 we have $(3\alpha^2+3\alpha+1)|(\alpha+4)\rightarrow(3\alpha^4+3\alpha^2+1)|(\alpha^2+4)$ but this means that $\alpha^2\equiv -4\equiv k^2$. Here $\lambda=5$ therefore $1\equiv\alpha^5\equiv k^5\rightarrow k^6\equiv k\equiv(-4)^4\equiv 18 \mod 41$. Using this k we have $5+2\alpha\rightarrow 5+36=41$. Therefore $5+2\alpha$ is divisible by $(3\alpha^4+3\alpha^2+1)$.

For α^2+2 we have $k^2\equiv -2\rightarrow k^6\equiv 3 \mod 11$ therefore $5+2\alpha\rightarrow 5+6=11$ and therefore $5+2\alpha$ is divisible by α^2+2. The quotient is a unit since as shown above $N(5+2\alpha)=11\cdot 41=N(\alpha^2+2)N(3\alpha^4+3\alpha^2+1)$.

Page 107, Problem 1 (d). We know that $N(5-4\alpha^2)=11\cdot 191$ and $N(\alpha+2)=11$ we also know that $\alpha\equiv -2 \mod \alpha+2$ therefore $5-4\cdot(-2)^2=-11\equiv 0 \mod 11$, therefore $5-4\alpha^2$ is divisible by $\alpha+2$. The norm of the quotient is obviously 191 as shown above.

Page 107, Problem 1 (e). We know that $2\alpha^4+\alpha^2+4|4\alpha-5$ therefore $4k\equiv 5 \mod 191$ and as shown in the book $k\equiv 49$. If we substitute $\alpha\rightarrow 49$ we do not get 0 mod 191 for $2\alpha^3+\alpha^4+4\equiv 29$, $2\alpha^2+\alpha+4\equiv 80$ and $2\alpha+\alpha^3+4\equiv 95$ therefore they are not divisible by $2\alpha^4+\alpha^2+4$.

Page 107, Problem 1 (f). The same thing over again, α^3+2 means that $k^3\equiv -2$ and $k\equiv k^6=(-2)^2\equiv 4 \mod 11$ therefore $\alpha+7\rightarrow 4+7=11\equiv 0 \mod 11$ and $\alpha+7$ is divisible by α^3+2.

From Page 98 we know that $k\equiv 49$ for $2\alpha^4+\alpha^2+4$, conjugating $\alpha\rightarrow\alpha^2$ we get $2\alpha^3+\alpha^4+4$ and $k^2\equiv 49$ therefore $k\equiv k^6\equiv 49^3\equiv -7 \mod 191$ therefore $\alpha+7\rightarrow -7+7\equiv 0 \mod 191$ and $\alpha+7$ is divisible by $2\alpha^3+\alpha^4+4$.

Page 107, Problem 1 (g). Again, the same scheme, $\alpha+2$ means that $k\equiv -2 \mod 11$ therefore $\alpha^4-5\rightarrow 16-5=11\equiv 0 \mod 11$ and therefore $\alpha+2$ divides α^4-5.

Page 107, Problem 2 (a). To check divisibility we need to find the corresponding k for $2\alpha^5+2\alpha^2+\alpha+1$. But this might not be easy, however, we can do the opposite, for example we can go from $3-2\alpha\equiv 0 \mod 71$ to get $\alpha\equiv -34 \mod 71$. Because if this k belongs to $2\alpha^5+2\alpha^2+\alpha+1$ then $2k^5+2k^2+k+1$ will be $0 \mod 71$ as $2\alpha^5+2\alpha^2+\alpha+1$

is obviously divisible by $2\alpha^5 + 2\alpha^2 + \alpha + 1$. And for $k \equiv -34$ it does, $2k^5 + 2k^2 + k + 1$ will be $0 \mod 71$.

We can then try all the conjugates of $3 - 2\alpha$ to see if the corresponding k will work on $2\alpha^5 + 2\alpha^2 + \alpha + 1$. Here $\lambda = 7$ therefore $k^8 \equiv k$. For $3 - 2\alpha^2$ we have $k^2 \equiv -34 \to k^8 \equiv k \equiv 45 \mod 71$ causing $2k^5 + 2k^2 + k + 1 \equiv 3 \mod 71$ a no go.

For $3 - 2\alpha^3$ we have $k^3 \equiv -34 \to k^{15} \equiv k \equiv 32 \mod 71$ causing $2k^5 + 2k^2 + k + 1 \equiv 41 \mod 71$ a no go.

For $3 - 2\alpha^4$ we have $k^4 \equiv -34 \to k^8 \equiv k \equiv 20 \mod 71$ causing $2k^5 + 2k^2 + k + 1 \equiv 29 \mod 71$ a no go.

For $3 - 2\alpha^5$ we have $k^5 \equiv -34 \to k^{15} \equiv k \equiv 30 \mod 71$ causing $2k^5 + 2k^2 + k + 1 \equiv 59 \mod 71$ a no go.

For $3 - 2\alpha^6$ we have $k^6 \equiv -34 \to k^{36} \equiv k \equiv 48 \mod 71$ causing $2k^5 + 2k^2 + k + 1 \equiv 11 \mod 71$ a no go.

According to the above $\alpha \equiv -34$ works it setting $2k^5 + 2k^2 + k + 1$ to be $0 \mod 71$. It's true that this is not conclusive this is more of the if part of an if and only if but we can still make it conclusive.

Calculating the norm $N(\alpha + 37)$ we get $1500667147 = 7 \cdot 29 \cdot 71 \cdot 104119$. This means that since $N(2\alpha^5 + 2\alpha^2 + \alpha + 1) = 71$ we have $2\alpha^5 + 2\alpha^2 + \alpha + 1$ dividing one of the conjugates of $(\alpha + 37)$.

From this point we can check all conjugates of $(\alpha + 37)$ and see what value k works for those conjugates but these values were listed above and the only one that worked for $2\alpha^5 + 2\alpha^2 + \alpha + 1$ was $k \equiv -37$ therefore $2\alpha^5 + 2\alpha^2 + \alpha + 1$ divides $\alpha + 37$ and by the Theorems on Page 92 its value of k is indeed $\equiv -37$ and it therefore divides $3 - 2\alpha$.

Page 107, Problem 2 (b). Just like in Part (a) we need to find the corresponding k, here $\alpha + 4 \to k \equiv -4$, so let's create the table (note also that $N(1 + \alpha^2 - \alpha^4) = 29$)

$$\begin{aligned}
\alpha &\to \alpha^2 \to 1 + k^4 - k \equiv 0 \mod 29 \\
\alpha &\to \alpha^3 \to 1 + k^6 - k^5 \equiv -12 \mod 29 \\
\alpha &\to \alpha^4 \to 1 + k - k^2 \equiv -19 \mod 29 \\
\alpha &\to \alpha^5 \to 1 + k^3 - k^6 \equiv 15 \mod 29 \\
\alpha &\to \alpha^6 \to 1 + k^5 - k^3 \equiv -2 \mod 29
\end{aligned}$$

in all those calculations we set $k \equiv -4$ we are not changing k. Thus the conjugate $\alpha \to \alpha^2$, *i.e.* $1 + \alpha^4 - \alpha$ is the one, again like Part (a) this is only the if of the if and only if but again we can make sure by calculating $N(\alpha + 4) = 3277 = 29 \cdot 113$ which means that $1 + \alpha^4 - \alpha$ divides one of the conjugates of $\alpha + 4$ we can then do the same test as in Part (a) to see which conjugates it divides and we will find out that it is $\alpha + 4$.

Now to the quotient

$$\frac{\alpha + 4}{1 + \alpha^4 - \alpha} = 2 + 2\alpha + 2\alpha^2 + 3\alpha^3 + 2\alpha^4 + \alpha^5$$

Page 107, Problem 2 (c). Here we need to calculate the norm, again I used my Python script but this time I enhanced the script to use Periods as given in the Footnote of Page 100 or more completely in Section 4.5. The catch with this is we need to first fins the primitive root mod λ and find e and f that minimizes $e + f$ where $ef = \lambda - 1$ this is because

$$Ng(\alpha) = G(\alpha) \cdot \sigma G(\alpha) \cdot \sigma^2 G(\alpha) \cdot \cdots \cdot \sigma^{e-1} G(\alpha)$$
$$G(\alpha) = g(\alpha) \cdot \sigma^e g(\alpha) \cdot \sigma^{e^2} g(\alpha) \cdot \cdots \cdot \sigma^{\lambda - 1 - e} g(\alpha)$$

So you see that there are $f - 1$ multiplications for $Ng(\alpha)$ and $e - 1$ multiplications for $G(\alpha)$, the python script is as follows

```
# the following two functions are used to generate primitive roots
# translated to Python from http://www.bluetulip.org/2014/programs/primitive.js
# (some rights may remain with the author of the above javascript code)

def isNotPrime(possible):
    i = 2
    while i <= possible**0.5:
        if (possible % i) == 0:
            return True
        i = i + 1
    return False

def primRoots(theNum):
    if isNotPrime(theNum):
        raise ValueError("Sorry, the number must be prime.")
    o = 1
    roots = []
    r = 2
    while r < theNum:
        k = pow(r, o, theNum)
        while (k > 1):
            o = o + 1
            k = (k * r) % theNum
        if o == (theNum - 1):
```

```
            roots.append(r)
        o = 1
        r = r + 1
    return roots
    min_tot = 2 + (L-1)/2
    min_e = 2

# search a factor e of L-1 such that e+f is minimized

def searchMinE(L):
    # we know we are searching a parabola and sqrt(L-1)
    # is the minimum point thus we break once we find the closest
    # integer factor but we search backwards and forwards

    if L <= 1:
        return L

    min_tot = 2 + (L-1)/2
    min_e = 2

    s = int(sqrt(L-1))
    for i in xrange(s,L):
        if ((L-1)% i) == 0:
            if (i + (L-1)/i) < min_tot:
                min_e = i
                min_tot = i + (L-1)/i
            break

    for i in xrange(s,0,-1):
        if ((L-1)% i) == 0:
            if (i + (L-1)/i) < min_tot:
                min_e = i
                min_tot = i + (L-1)/i
            break

    return min_e

# funtion to do sigma conjugation
def sigmaShift(f, g, k):
    L = len(f)
    return cycShift(f, pow(g,k,L))

# compute norm of f(A) using periods
# total e + f multiplications rather than e*f
# but first you must find a primitive root so the total
# time needed might be the same
def cycNormFast(f, g, e=2):

    # Find primitive a root
    # Create the \sigma operator \alpha \to \alpha^\gamma
    # Construct G(\alpha)
    # Multiply the G(\alpha)'s

    L = len(f)
    if L <= 1:
        return

    #g = primRoots(L)[0]
```

```
    # for now set e = 2
    # e = 2
    F = (L-1)/e

    # now construct G
    G = [i for i in f] # deep copy of f

    for k in xrange(1,F):
        fk = sigmaShift(f, g, k*e)
        G = multCyc(G, fk)

    # now construct G
    res = [i for i in G] # deep copy of f

    for k in xrange(1,e):
        Gk = sigmaShift(G, g, k)
        res = multCyc(res, Gk)

    #print res

    for k in xrange(3,L):
        if res[k] != res[k-1]:
            return

    return res[0] - res[1]
```

so for this problem the call would be like so, yielding a result of 197.

```
cycNormFast([2,0,2,0,0,0,1], g=primRoots(7)[0], e=searchMinE(7))
```

Page 107, Problem 2 (d). Again using the Python script above with the result of $1576 = 8 \cdot 197$.

```
cycNormFast([3,0,0,0,-1,0,-1], g=primRoots(7)[0], e=searchMinE(7))
```

Page 107, Problem 2 (e). We want to find an element with norm 8. Part (d) gives us some clue since the norm of $3 - \alpha^4 - \alpha^6$ is $8 \cdot 197$. From Page 101 we know that $\alpha^6 - 2\alpha^3 + \alpha + 1$ has norm 197 and it also has $\alpha \equiv k \equiv -6$. Now we need to find out which conjugate of $3 - \alpha^4 - \alpha^6$ is divisible by $\alpha^6 - 2\alpha^3 + \alpha + 1$.

It turned out that $3 - \alpha^6 - \alpha^2 \to 3 - 6^6 - 6^2 \equiv 0 \mod 197$. So we can divide this by $\alpha^6 - 2\alpha^3 + \alpha + 1$ using the usual algorithm (note that long division does not yield anything in this case) and we found that $\alpha^6 - \alpha^4 + \alpha^3$ or (factoring out the unit) $\alpha^3 - \alpha + 1$ has norm 8.

Page 107, Problem 3 (a). I think the first thing to do before factoring these cyclotomic integer is to find their norms, again I'll use the Python script above to get $N(5\alpha^4 - 3\alpha^3 - 5\alpha^2 + 5\alpha - 2) = 9455 = 5 \cdot 31 \cdot 61$

$N(\alpha-1)=\lambda=5$ so that's one factor, no need to see which conjugate because here $\alpha\equiv 1$ and $5-3-5+5-2\equiv 0 \mod 5$. Now we need to divide

$$\frac{5\alpha^4-3\alpha^3-5\alpha^2+5\alpha-2}{\alpha-1}=5\alpha^3+2\alpha^2-3\alpha+2$$

with norm $N(5\alpha^3+2\alpha^2-3\alpha+2)=1891=31\cdot 61$. Next use the fact that $N(2-\alpha)=31$ and we need to find which conjugate is divisible by $(2-\alpha)$ or the other way round we can find out which conjugate of $2-\alpha$ divides $5\alpha^3+2\alpha^2-3\alpha+2$ (this is less effort as we just need to find the new k while conjugating the longer cyclotomic integer takes more time). The answer is $2-\alpha^2$ so we divide again

$$\frac{5\alpha^3+2\alpha^2-3\alpha+2}{2-\alpha^2}=\alpha^3+\alpha^2-2\alpha+1$$

and just as a check $N(\alpha^3+\alpha^2-2\alpha+1)=61$. Thus

$$5\alpha^4-3\alpha^3-5\alpha^2+5\alpha-2=(\alpha-1)(2-\alpha^2)(\alpha^3+\alpha^2-2\alpha+1)$$

Page 107, Problem 3 (b). Just like Part (a) first calculate the norm $N(-4\alpha^3-11\alpha^2+8\alpha+15)=128161=11\cdot 61\cdot 191$ but we know that $N(2+\alpha)=11$, just need to find out which conjugate. It turned out to be $2+\alpha^3$ dividing

$$\frac{-4\alpha^3-11\alpha^2+8\alpha+15}{2+\alpha^3}=-3\alpha^3+11\alpha+13$$

as a consistency check the norm is $N(-3\alpha^3+11\alpha+13)=11651=61\cdot 191$. Again we know that $N(3+\alpha)=61$ need to find out which conjugate, it is $3+\alpha$ actually, dividing

$$\frac{-3\alpha^3+11\alpha+13}{3+\alpha}=-\alpha^3-\alpha^2+2\alpha+4$$

with norm $N(-\alpha^3-\alpha^2+2\alpha+4)=191$ thus

$$-4\alpha^3-11\alpha^2+8\alpha+15=(2+\alpha^3)(3+\alpha)(-\alpha^3-\alpha^2+2\alpha+4)$$

Page 107, Problem 4 (a). Same thing as Problem 3, norm $N(\alpha^2-3\alpha-4)=5461=43\cdot 127$ we know that $N(2+\alpha)=43$ the conjugate that divides is $2+\alpha^4$ dividing we get

$$\frac{\alpha^2-3\alpha-4}{2+\alpha^4}=\alpha^5+\alpha^4-2\alpha-2$$

with norm $N(\alpha^5+\alpha^4-2\alpha-2)=127$ thus

$$\alpha^2-3\alpha-4=(2+\alpha^4)(\alpha^5+\alpha^4-2\alpha-2)$$

Page 107, Problem 4 (b). Norm $N(\alpha^5 - \alpha^4 - 3\alpha^2 - 3\alpha - 2) = 1247 = 29 \cdot 43$ and $N(2+\alpha) = 43$ (I choose to use 43 first because from Kummer's table $29 = N(1+\alpha-\alpha^2)$). The conjugate that works is $(2 + \alpha^6)$ with

$$\frac{\alpha^5 - \alpha^4 - 3\alpha^2 - 3\alpha - 2}{2 + \alpha^6} = -\alpha^4 - 2\alpha^2 - \alpha - 1$$

but $N(-\alpha^4 - 2\alpha^2 - \alpha - 1) = 29$ so we are done

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

Page 107, Problem 5. We are just dividing (numerator is Kummer's denominator is the book's)

$$\frac{2 + \alpha + \alpha^3}{2\alpha^5 + 2\alpha^2 + \alpha + 1}$$

but this turns out not to work because it's the conjugate $\alpha \to \alpha^5$, *i.e.* $2 + \alpha + \alpha^5$ that is actually divisible by $2\alpha^5 + 2\alpha^2 + \alpha + 1$ with the quotient $-\alpha^4 - \alpha^3 - \alpha^2 - \alpha$ and this is a unit.

Page 107, Problem 6. We want to find an element with $\lambda = 19, p = 191$, again in this case I wrote a Python script to implement the algorithm in the book as follows

```
# calculate prime factor for primes that divide a binomial
def binPrimeFactor(L, p):
    if (p-1) % L != 0:
        return

    w = (p-1) / L
    k = pow(2, w, p)

    # calculate all powers of k
    kp = [pow(k, i, p) for i in xrange(L)]

    # calculate all g(\alpha) made of two powers of k
    # there are four possibilities with plus minus for each

    # prepare things for cycNormFast
    g = primRoots(L)[0]

    # this part is to find e and f that minimizes e + f
    # so that we minimize the number of multiplication
    # in the cycNormFast function

    min_e = searchMinE(L)
    print min_e

    # now we generate all combos for powers of k
    import itertools
```

```
t = [i for i in range(1,L)]
for u in xrange(2,L):

    l = itertools.combinations(t, u)

    for i in l:
        # create a bitmap for the plus minus
        for k in range(0,2**u):
            res = [0] * L
            for j in range(u):
                b = pow(-1,(k >> j) & 0x01)
                res[i[j]] = b*1
                res[0] -= b*kp[i[j]]
            N = cycNormFast(f=res, g=g, e=min_e)
            if N == p:
                print N, res, u
```

and the results are many :) the first one is $\alpha^9 - \alpha^4 - 1$ compared to Kummer's $1 + \alpha + \alpha^{16}$.

Page 107, Problem 7. Constructing more entries in Kummer's table, we can continue with $p = 191$ or continue with more prime, the next three after 761 are $1103, 1217, 1483$

$$N(\alpha^8 - \alpha^3 + \alpha^2 + 1) = 1217$$
$$N(\alpha^{11} - \alpha - 1) = 1483$$
$$N(\alpha^{16} - \alpha^{11} - \alpha^5 + \alpha + 1) = 1559$$

I couldn't find a factorization of 1103 so I calculated the next one 1559. So I tried doing the same thing to 1103 as what was done on the book for 47 with $\lambda = 23$, from Section 4.5 what this means is we are setting $e = 2$ and periods with length $f = (\lambda - 1)/e = (19 - 1)/2 = 9$. The periods are given by

$$\theta_0 = \alpha^1 + \alpha^4 + \alpha^{16} + \alpha^7 + \alpha^9 + \alpha^{17} + \alpha^{11} + \alpha^6 + \alpha^5$$
$$\theta_1 = \alpha^2 + \alpha^8 + \alpha^{13} + \alpha^{14} + \alpha^{18} + \alpha^{15} + \alpha^3 + \alpha^{12} + \alpha^{10}$$

with the same identities $\theta_0 + \theta_1 = 1$, this means that $Nf(\alpha) = F(\alpha) \cdot \sigma F(\alpha)$ with $F(\alpha) = f(\alpha) \cdot \sigma^2 f(\alpha) \cdot \sigma^4 f(\alpha) \cdot \sigma^6 f(\alpha) \cdot \cdots \cdot \sigma^{16} f(\alpha) = a + b\theta_0$ and therefore $\sigma F(\alpha) = a + b\theta_1$ and

$$Nf(\alpha) = (a + b\theta_0)(a + b\theta_1)$$

Calculated this one by hand to get

$$\theta^2 = \theta_1 - 4$$
$$\rightarrow \theta_0\theta_1 = \theta_0(-1-\theta_1) = 5$$
$$\rightarrow 1103 = (a+b\theta_0)(a+b\theta_1) = a^2 - ab + 5b^2$$

and as what was done in the book, multiply everything by 4 to get

$$4412 = (2a-b)^2 + 19b^2$$

The curious thing here is that the coefficient of b^2 is $\lambda = 19$ while in the book it is $\lambda = 23$, it seems like the coefficient of b^2 should be λ :) So here I also tried different b's from 1 to 15, only one b works, which is 7

$$4412 - 19 \cdot 7^2 = 59^2 = (2a-7)^2$$
$$\rightarrow a = 33$$

and so $F(\alpha) = 33 + 7\theta_0$, the question now is if we can concoct an $f(\alpha)$ such that $F(\alpha) = 33 + 7\theta_0$. ¯\(°_o)/¯

Page 107, Problem 8. I did not follow the hint but I calculated $N(1+\alpha-\alpha^7+\alpha^8+\alpha^{11}) = 547$ and not 599 so it must be wrong :)

Page 107, Problem 9. The condition $f(\alpha) = f(-\alpha)$ means

$$f(\alpha) = a_0 + a_1(\alpha+\alpha^{-1}) + a_2(\alpha^2+\alpha^{-2}) + \cdots + a_{11}(\alpha^{11}+\alpha^{-11})$$

setting $\alpha \rightarrow 4$ we get

$$f(4) \equiv a_0 + 16a_1 + 19a_2 + 6a_3 + 30a_4 + 4a_5 + 34a_6 + 23a_7 + 5a_8 + 10a_9 + 14a_{10} + 26a_{11}$$

we require $f(\alpha) \equiv 0 \mod 47$ because $N(\alpha-4) = 23456248059221 = 47 \cdot 178481 \cdot 2796203$ so if 47 has a prime factor it must divide $\alpha - 4$ and therefore $\alpha \equiv 4$. Note, however, that Kummer's factor of $\alpha^{10}+\alpha^{-10}+\alpha^8+\alpha^{-8}+\alpha^7+\alpha^{-7}$ doesn't satisfy this condition, replacing α with 4 we get $42 \mod 47$. This might mean that it was it's conjugate that is divisible by the "ideal" factor of 47, let's see if this is true with the following simple Python script

```
# calcule f(k) mod p given f(\alpha)
def calcFK(f, k, p):
    L = len(f)

    res = 0
    for i in range(L):
        res += f[i]*pow(k,i,p)

    return res % p

# find if a conjugate of f(\alpha) satisfies f(k) \equiv 0 \mod{p}
def findConjWithCorrectK(f, k, p):

    L = len(f)
    for i in xrange(1, L):
        if calcFK(cycShift(f, i), k, p) == 0:
            print i
```

the answer is that $\alpha \to \alpha^{10}$ and $\alpha \to \alpha^{13}$ satisfy $f(4) \equiv 0 \mod 47$.

To get a few simple candidates we can set some of them to zero but I think it's easier to write a Python script as it's very similar to the one used to find a prime factor above, Problem 6, this one is

```
def findSquarePrime(L, a, p):

    hl = (((L-1)/2) + 1)
    kp = [1] * hl
    for i in xrange(1,hl):
        kp[i] = (pow(a,i,p) + pow(a,L-i,p)) % p

    print kp

    g = primRoots(L)[0]
    min_e = searchMinE(L)

    import itertools
    t = [i for i in range(1,hl)]

    for u in xrange(2,hl):

        l = itertools.combinations(t, u)

        for i in l:
            # create a bitmap for the plus minus
            for k in range(0,2**u):
                res = [0] * L
                for j in range(u):
                    b = pow(-1,(k >> j) & 0x01)
                    res[i[j]] = b*1
                    res[L-i[j]] = b*1
                    res[0] -= 2*b*kp[i[j]]
                N = cycNormFast(f=res, g=g, e=min_e)
                if N == p**2:
                    print N, res, u
```

```
# use case
findSquarePrime(23, 4, 47)
```

There are many solution, the first one is

$$\begin{aligned} f(\alpha) &= -(\alpha^1 + \alpha^{-1}) + (\alpha^3 + \alpha^{-3}) + (\alpha^9 + \alpha^{-9}) \\ \rightarrow f(4) &\equiv -16 + 6 + 10 \equiv 0 \mod 47 \end{aligned}$$

but the questions asks for a few solutions so here are a couple more

$$\begin{aligned} f(\alpha) &= 2 - (\alpha^2 + \alpha^{-2}) + (\alpha^5 + \alpha^{-5}) + (\alpha^{10} + \alpha^{-10}) \\ f(\alpha) &= -(\alpha^2 + \alpha^{-2}) + (\alpha^8 + \alpha^{-8}) + (\alpha^{10} + \alpha^{-10}) \end{aligned}$$

As noted earlier Kummer's solution satisfies $f(4) \equiv 0 \mod 47$ only if we take the conjugate $\alpha \rightarrow \alpha^{10,13}$, the norm of the solutions above are all guaranteed to be $p^2 = 47^2$ as that's how the script works.

Page 107, Problem 10. We need to prove that if λ divides $Ng(\alpha)$ then $\alpha - 1$ divides $g(\alpha)$. We know that $\lambda = N(\alpha - 1) | Ng(\alpha)$, which is the assumption of the problem. But since $\alpha - 1$ is prime as shown in the Corollary of Page 93, it must divide one of the conjugates of $g(\alpha)$, say $\alpha - 1 | g(\alpha^j)$.

But since λ is prime there must be an integer i such that $ij \equiv 1 \mod \lambda$, therefore $\alpha - 1 | g(\alpha^j) \rightarrow \alpha^i - 1 | g(\alpha^{ij}) = g(\alpha)$ but $\alpha^i - 1 = (\alpha - 1)(\dots)$, thus $\alpha - 1 | g(\alpha)$.

Page 107, Problem 11. We can do it in an easy way or a harder way. The easy way is to just multiply $\alpha - 1$ with $1 + 2\alpha + 3\alpha^2 + \cdots + \lambda\alpha^{\lambda-1}$ and see that the result is

$$\begin{aligned} (1-2)\alpha + (2-3)\alpha^2 + \cdots + (\lambda - 1 - \lambda)\alpha^{\lambda-1} + \lambda - 1 &= \lambda - 1 - (\alpha + \alpha^2 + \cdots + \alpha^{\lambda-1}) \\ &= \lambda - 1 + 1 = \lambda \end{aligned}$$

The harder way is to do long division on $N(\alpha - 1)$ by $\alpha - 1$ to get $(\alpha^2 - 1)(\alpha^3 - 1) \dots (\alpha^{\lambda-1} - 1)$. But first we need to massage $N(\alpha - 1) = \lambda \rightarrow \alpha^{\lambda-1} + \alpha^{\lambda-2} + \cdots + (1 + \lambda)$.

$$
\begin{array}{r|l}
\alpha - 1 & \alpha^{\lambda-2} + 2\alpha^{\lambda-3} + 3\alpha^{\lambda-4} + 4\alpha^{\lambda-5} + \quad \ldots \quad + (\lambda - 1) \\
\sqrt{} & \alpha^{\lambda-1} + \alpha^{\lambda-2} + \ \alpha^{\lambda-3} + \ \alpha^{\lambda-4} + \ \alpha^{\lambda-5} + \quad \ldots \quad + (1 + \lambda) \\
& \alpha^{\lambda-1} - \alpha^{\lambda-2} \\
\hline
& 2\alpha^{\lambda-2} + \alpha^{\lambda-3} \\
& 2\alpha^{\lambda-2} - 2\alpha^{\lambda-3} \\
\hline
& 3\alpha^{\lambda-3} + \ \alpha^{\lambda-4} \\
& 3\alpha^{\lambda-3} - 3\alpha^{\lambda-4} \\
\hline
& 4\alpha^{\lambda-4} + \ \alpha^{\lambda-5} \\
& 4\alpha^{\lambda-4} - 4\alpha^{\lambda-5} \\
\hline
& \vdots \\
\hline
& (\lambda - 1)\alpha + (\lambda + 1) \\
& (\lambda - 1)\alpha - (\lambda - 1) \\
\hline
& 2\lambda
\end{array}
$$

Therefore

$$
\begin{aligned}
\frac{\lambda}{\alpha - 1} &= \alpha^{\lambda-2} + 2\alpha^{\lambda-3} + 3\alpha^{\lambda-4} + 4\alpha^{\lambda-5} + \cdots + (\lambda - 1) + \frac{2\lambda}{\alpha - 1} \\
\rightarrow \frac{\lambda}{\alpha - 1} &= -\alpha^{\lambda-2} - 2\alpha^{\lambda-3} - 3\alpha^{\lambda-4} - 4\alpha^{\lambda-5} - \cdots - (\lambda - 1) \\
&= \lambda\alpha^{\lambda-1} + (\lambda - 1)\alpha^{\lambda-2} + (\lambda - 2)\alpha^{\lambda-3} + (\lambda - 3)\alpha^{\lambda-4} + (\lambda - 4)\alpha^{\lambda-5} + \ldots 1
\end{aligned}
$$

we get to the last line by adding $\lambda(\alpha^{\lambda-1} + \alpha^{\lambda-2} + \cdots + 1)$.

Page 107. Summary of Section 4.5

1. The introduction of the operator σ is an actually good move. For example $\sigma^2 \cdot \sigma^3 = \sigma^5$ so we can threat them like normal numbers w.r.t. exponents. The catch is that one, its operation on α is quite complex $\sigma f(\alpha^j) = f(\alpha^{\gamma^j})$. The next catch is that operation on periods must be handled carefully $\sigma^i \eta_1 \eta_2 = \eta_{1+i}\eta_{2+i}$, it applies to both periods and not just $(\sigma^i \eta_1)\eta_2$.

2. The periods, η_i, is made of repeated applications of σ, *i.e.* to create a period take a power of alpha, α^j, and then

$$\eta_i = \alpha^j + \sigma^e \alpha^j + \sigma^{2e} \alpha^j + \cdots + \sigma^{-e} \alpha^j$$

   This applies to **any** period, for η_0 we have to start with α we can start with any α^j but it must contain α at the end so it's easier to start with α.

Page 109. Top page, proof that periods are independent of the choice of primitive roots. First it says "if α^j is any power of α, and if η_i is the period which contains it, then η_i also contains $\sigma'^e\alpha^j$. (Then it also contains $\sigma'^e\sigma'^e\alpha^j = \sigma'^{2e}\alpha^j, \sigma'^{3e}\alpha^j, \ldots, \sigma'^{-e}\alpha^j$".

The note in bracket is just the consequence of the previous if, what it says is first we need to establish that if α^j is in η_i then $\sigma^e\alpha^j$ is also in η_i. Once this is established we note that $\sigma^e\alpha^j$ is just α^k for some k but by the application of the if statement α^k in η_i means that $\sigma^e\alpha^k = \sigma^{2e}\alpha^j$ is also in η_i and we can repeat the argument again and again.

Page 109. Top page, continuation of the above proof, "suffice to prove that σ'^e is a power of σ^e". To see this, the first key is to note that any period can be expressed as sums of powers of σ^e with the appropriate choice of α^j

$$\begin{aligned}\eta_i &= \alpha^j + \sigma^e\alpha^j + \sigma^{2e}\alpha^j + \cdots + \sigma^{-e}\alpha^j \\ &= \sum_{s=0}^{f-1} \sigma^{se}\alpha^j\end{aligned}$$

where $\sigma^{efn} = 1$ for any integer n (this is the other key). The problem I had was that say $\sigma'^e = \sigma^{me}$, how do we know that σ^{me} is one of those σ^{se}? Easy, this is because $\sigma^{efn} = 1$ so we just need $m \mod f$, let $l \equiv m \mod f$ then $\sigma^{me} = \sigma^{le}$ with $0 \leq l < f$ but s runs from $0 \leq s < f$ thus we are guaranteed to find a value of s such that $s \equiv m \mod f$.

Page 110, Problem 1. Since $\lambda = 5$, $e = 2$ means that $f = (\lambda - 1)/2 = 2$. The primitive roots of 5 are 2 and 3. Let's choose 2 as our primitive root. In this case we only have θ_0 and θ_1

$$\begin{aligned}\theta_0 &= \alpha + \sigma^2\alpha = \alpha + \alpha^4 \\ \theta_1 &= \sigma\theta_0 = \alpha^2 + \alpha^3\end{aligned}$$

The multiplication table is

$$\begin{aligned}\theta_0^2 &= \alpha^2 + \alpha^3 + 2 = \theta_1 + 2 \\ \theta_0\theta_1 &= -\theta_0 - \theta_0^2 \\ &= -\theta_0 - \theta_1 - 2 \\ &= 1 - 2 = -1\end{aligned}$$

Next we need to find a cyclotomic integer whose norm is divisible by a prime that is neither 1 nor 0 mod 5. From page 108 we know that $Ng(\alpha) = G(\alpha)G(\alpha^2)$ and

$G(\alpha) = a + b\theta_0$ (we can always eliminate θ_1 by using $\theta_0 + \theta_1 = 1$), therefore the norm is given by $(a + b\theta_0)(a + b\theta_1) = a^2 - ab - b^2$. there are plenty values for a and b that generate a prime factor $\not\equiv 0, 1 \mod 5$ a few of them are $(a, b, p) = (5, 1, 19), (6, 1, 29), (7, 3, 19), (9, 2, 59), (9, 4, 29), (11, 1, 109), (11, 3, 79)$ where p is the prime factor of the norm.

But the problem now is that we need to find $g(\alpha)$ (note what we have now is $G(\alpha)$ and not $g(\alpha)$) such that we get the values of a and b above. Note that we can also cast it in terms of $m\theta_0 + n\theta_1$ by eliminating the constant using $-1 = \theta_0 + \theta_1$. In this case we get $Ng(\alpha) = -m^2 + 3mn - n^2$ with more or less the same result.

But of course we can "cheat" instead of trying to find the actual $g(\alpha)$ that generates the above a and b if we just set $g(\alpha) = 2$ then $Ng(\alpha) = 16$ or if $g(\alpha) = 7$ then $Ng(\alpha) = 7^4$ and the prime factor of the norm is obviously $\not\equiv 0, 1 \mod 5$:)

From Page 96, Problem 5, if p divides the norm of a binomial then $p \equiv 0, 1 \mod \lambda$, since this is not the case then we can't deploy the mechanism in Section 4.4 to find its prime cyclotomic factors.

Page 110, Problem 2. We need to show that the form of $Nf(\alpha)$ for $\lambda = 7$ is $\frac{1}{4}[A^2 + 7B^2]$. The key of course is to choose $e = 2$ so that we only have two periods θ_0 and θ_1. In which case the period length is $f = 3$.

If this is the case then the norm is given by

$$\begin{aligned} Nf(\alpha) &= (a\theta_0 + b\theta_1)(a\theta_1 + b\theta_0) \\ &= (a^2 + b^2)\theta_0\theta_1 + ab(\theta_0^2 + \theta_1^2) \end{aligned}$$

so what we need is $\theta_0\theta 1$ and $\theta_0^2 + \theta_1^2$ the smallest primitive root mod 7 is 3 so

$$\begin{aligned} \theta_0 &= \alpha + \alpha^{3^2} + \alpha^{3^4} \\ &= \alpha + \alpha^2 + \alpha^4 \\ \theta_1 &= \alpha^3 + \alpha^5 + \alpha^6 \\ \theta_0\theta_1 &= 3 + \theta_0 + \theta_1 \\ &= 2 \end{aligned}$$

and also

$$\begin{aligned}(-1)^2 = (\theta_0+\theta_1)^2 &= (\theta_0^2+\theta_1^2)+2\theta_0\theta_1\\ 1 &= (\theta_0^2+\theta_1^2)+4\\ -3 &= (\theta_0^2+\theta_1^2)\end{aligned}$$

since $\theta_0+\theta_1=-1$. Thus

$$Nf(\alpha) = 2a^2-3ab+2b^2$$

Let $a+b=u, a-b=v$ and

$$\begin{aligned}2a^2-3ab+2b^2 &= \tfrac{1}{4}\{2(u+v)^2-3(u^2-v^2)+2(u-v)^2\}\\ &= \tfrac{1}{4}\{u^2+7v^2\}\end{aligned}$$

I initially tried $Nf(\alpha)=(a+b\theta_0)(a+b\theta_1)=a^2-ab+2b^2$ but $a+b=u, a-b=v$ doesn't gibe us much as the substitution yields $\frac{1}{4}(2u^2-2uv+4v^2)$.

Page 110, Problem 3. We want to calculate $(\theta_0-\theta_1)^2$ for several values of λ,

$$\begin{array}{lll}
\lambda = 3 \rightarrow (\theta_0-\theta_1)^2 = -3 & \frac{\lambda-1}{2} = 1\\
\lambda = 5 \rightarrow (\theta_0-\theta_1)^2 = 5 & \frac{\lambda-1}{2} = 2\\
\lambda = 7 \rightarrow (\theta_0-\theta_1)^2 = -7 & \frac{\lambda-1}{2} = 3\\
\lambda = 11 \rightarrow (\theta_0-\theta_1)^2 = -11 & \frac{\lambda-1}{2} = 5\\
\lambda = 13 \rightarrow (\theta_0-\theta_1)^2 = 13 & \frac{\lambda-1}{2} = 6\\
\lambda = 17 \rightarrow (\theta_0-\theta_1)^2 = 17 & \frac{\lambda-1}{2} = 8\\
\lambda = 19 \rightarrow (\theta_0-\theta_1)^2 = -19 & \frac{\lambda-1}{2} = 9\\
\lambda = 23 \rightarrow (\theta_0-\theta_1)^2 = -23 & \frac{\lambda-1}{2} = 11\\
\lambda = 29 \rightarrow (\theta_0-\theta_1)^2 = 29 & \frac{\lambda-1}{2} = 14\\
\lambda = 31 \rightarrow (\theta_0-\theta_1)^2 = -31 & \frac{\lambda-1}{2} = 15
\end{array}$$

So it seems like the formula is

$$(\theta_0-\theta_1)^2 = (-1)^{\frac{\lambda-1}{2}}\lambda$$

The Python script I used to calculate the above numbers is

```
def Problem3(L):
    g = primRoots(L)[0]
    e = 2
    f = (L-1)/e

    t = [0] * L

    for i in xrange(f):
        t[pow(g,i*e,L)] = 1

    for i in xrange(f):
        t[pow(g,(i*e) + 1,L)] = -1

    res = multCyc(t,t)
    return res[0] - res[1]
```

Page 110, Problem 4. We now need to prove the formula we found in Problem 3. To do this let's list a few facts we'll need

1. **Proposition 110.0** A cyclotomic integer is invariant under σ^e if and only if it is made of periods and constants.

   Proof. The constant part is obvious. The only if part is easy, if it's made of periods it's of course invariant under σ^e. The other way is also easy. To be invariant under σ^e means that if any α^j is part of the cyclotomic integer $\sigma^e\alpha^j$ must be in as well which in turn means that since $\sigma^e\alpha^j = \alpha^k$ is in then $\sigma^e\alpha^k = \sigma^{2e}\alpha^j$, etc are also in. But this is the definition of periods $\eta_i = \sum_{u=0}^{f-1} \sigma^{ue}\alpha^j$ and we are done :)

   In other words products and sums and product of sums and sums of products of periods (and other combinations) are also a period. We need this fact because we want to express $\theta_0^2 = a\theta_0 + b\theta_1$ (only in terms of periods), we can always remove the constant term (or any period θ_i) using the identity $\theta_0 + \theta_1 = -1$.

2. We need to simplify what we want $(\theta_0 - \theta_1)^2$ into

$$(\theta_0 - \theta_1)^2 = (\theta_0 - (-1 - \theta_1))^2 = (2\theta_0 + 1)^2$$
$$= 4(\theta_0^2 + \theta_0) + 1$$

   we could have eliminated θ_0 and get $(\theta_0 - \theta_1)^2 = 4(\theta_1^2 + \theta_1) + 1$.

3. No.1 above shows that (as mentioned earlier) we can express

$$\begin{aligned}\theta_0^2 &= a\theta_0 + b\theta_1 \\ \rightarrow \sigma\theta_0^2 &= \theta_1^2 = a\theta_1 + b\theta_0\end{aligned}$$

The identity $(\theta_0 - \theta_1)^2 = 4(\theta_0^2 + \theta_0) + 1 = 4(\theta_1^2 + \theta_1) + 1$ gives

$$\begin{aligned}4(\theta_0^2 + \theta_0) + \cancel{1} &= 4(\theta_1^2 + \theta_1) + \cancel{1} \\ a\theta_0 + b\theta_1 + \theta_0 &= a\theta_1 + b\theta_0 + \theta_1 \\ \rightarrow [(a+1) - b]\theta_0 &= [(a+1) - b]\theta_1\end{aligned}$$

but we know that $\theta_0 \neq \theta_1$ so it means that $(a+1) - b = 0 \rightarrow \theta_0^2 = a\theta_0 + (a+1)\theta_1$ and

$$\begin{aligned}(\theta_0 - \theta_1)^2 &= 4(\theta_0^2 + \theta_0) + 1 \\ &= -4(a+1) + 1\end{aligned}$$

We now need to find the value of a as a function of λ.

4. From Problem 3 we know that $\frac{\lambda-1}{2}$ plays an important role and it does. We can split the proof to two cases, one where $\frac{\lambda-1}{2}$ is even and the other where it is odd. The important thing about this is that when $\frac{\lambda-1}{2}$ is even we have -1 to be a quadratic residue, otherwise it is a quadratic non residue.

5. The main idea of the proof is to count the multiplicity of periods θ_0 and θ_1 in θ_0^2, we know that

$$\begin{aligned}\theta_0 &= \sum_{u=0}^{f-1} \sigma^{ue}\alpha \\ \rightarrow \theta_0^2 &= \left(\sum_{u=0}^{f-1} \sigma^{ue}\alpha\right)^2 \\ &= \left(\sum_{u=0}^{f-1} \sigma^{ue}\alpha^2\right) + 2 \times \{\text{cross terms}\}\end{aligned}$$

Note that $(\sigma^{ue}\alpha^j)^2 = \sigma^{ue}\alpha^{2j}$, this is how we got the first term in the RHS and let's call it the main term M. Since we have only two periods, this main term can only be either θ_0 or θ_1 but let's just call it M for now.

Let's check the cross terms. In squaring a sum the cross terms are made from

$$(a+b+c+d)^2 \to (2ab+2ac+2ad)+(2bc+2bd)+(2cd)$$

therefore in the example above there are $2\times(3+2+1)$ cross terms. In our case, our periods have length $f=\frac{\lambda-1}{2}$, therefore there are $2\times((f-1)+(f-2)+\cdots+1) = 2\times\frac{f(f-1)}{2}$ cross terms. From No.1 we know that they must form periods. Since each period has f terms there must be at most $f-1$ periods.

The at most part comes into play because some of the cross terms can be $\alpha^\lambda = 1$, we now need to know under what circumstances that this happens and how many they are.

Let's denote a primitive root mod λ as β then we can express

$$\theta_0 = \sum_{ue}^{f-1} \alpha^{\beta^{ue}}$$

a cross term would like like $\alpha^{\beta^{u_1 e}+\beta_{u_2 e}}$ where we can assume that $u_1 < u_2$ therefore if we want a cross term to be α^λ we must have

$$\begin{aligned} \alpha^{\beta^{u_1 e}+\beta_{u_2 e}} &= 1 \\ \to \beta^{u_1 e}+\beta_{u_2 e} &\equiv 0 \mod \lambda \\ \beta^{u_1 e}(1+\beta^{(u_2-u_1)e}) &\equiv 0 \mod \lambda \end{aligned}$$

or in other words $-1 \equiv \beta^{(u_2-u_1)e}$ but here $e=2$ therefore it means that -1 must be a quadratic residue since it is an even power of a primitive root. And as shown above it is also a sufficient condition, if -1 is not a quadratic residue than none of the cross term can be α^λ.

The question now is how many of the cross terms are α^λ? $-1 \equiv \beta^{ke}$ means that $1 \equiv \beta^{2ke}$ but since β is a primitive root this means that $2ke = 2f \to k = \frac{f}{2}$ (recall

that $e = 2$). Thus the only combinations that produce α^λ are

$$\alpha^{\beta^0} \cdot \alpha^{\beta^{ke}}, \alpha^{\beta^e} \cdot \alpha^{\beta^{(k+1)e}}, \alpha^{\beta^{2e}} \cdot \alpha^{\beta^{(k+2)e}}, \ldots$$

but $k = \frac{f}{2}$ and the sum $\theta_0 = \sum_{ue}^{f-1} \alpha^{\beta^{ue}}$ runs only to $f - 1$ therefore there are only

$$(f-1) - \frac{f}{2} + 1 = \frac{f}{2}$$

cross terms that produce α^λ. The plus 1 is because the $f - 1$ term is also included. There can be no other combinations, this can be shown easily by contradiction because otherwise $\beta^{w_1 e}(1 + \beta^{(w_2 - w_1)e}) \equiv 0 \mod \lambda$ then $-1 \equiv \beta^{(w_2 - w_1)e}$ but since β is a primitive root we must have $w_2 - w_1 = k$. The only thing we forgot was the factor of 2 multiplying all the cross terms, therefore there are in total $2 \times \frac{f}{2} = f$ terms of $\alpha^\lambda = 1$.

6. Let's recap, there are $f(f-1)$ cross terms and f of them are $\alpha^\lambda = 1$ therefore there are only $f(f-2)$ terms available to form periods and since each period has f terms we have exactly $f - 2$ periods. Therefore

$$\theta_0^2 = A\theta_0 + B\theta_1 + C$$

where $A + B = f - 2 + 1$ (the total number of periods, the plus one is from the main term that we've not touched till now) and $C = f$ (the total number of $\alpha^\lambda = 1$). But from No. 3 above we know that if we remove the constant term, here it is C, we must have $\theta_0^2 = a\theta_0 + (a+1)\theta_1$. Therefore what we have is

$$(A - C) = a, \quad (B - C) = a + 1 \qquad \rightarrow \qquad B = A + 1$$

with $A + B = f - 1$ and $C = f$, solving we get

$$\begin{aligned} 2B - 1 &= f - 1 \\ \rightarrow B &= \frac{f}{2} \\ \rightarrow A &= \frac{f}{2} - 1 \end{aligned}$$

and $a = A - C = -\frac{f}{2} - 1$ and

$$\begin{aligned}(\theta_0 - \theta_1)^2 &= -4(a+1) + 1 \\ &= 2f + 1 = \lambda\end{aligned}$$

recall that $f = \frac{\lambda-1}{2}$. This is what we want for even $f = \frac{\lambda-1}{2}$. Lastly, for odd $f = \frac{\lambda-1}{2}$, as explained above we do not have α^λ in the cross terms therefore $f(f-1)$ cross terms all form periods and there are $f-1$ periods

$$\theta_0^2 = A\theta_0 + B\theta_1$$

with $A + B = f - 1 + 1$ (again the plus one is from the main term) and it must be that $B = A + 1$ (as dictated by No. 3), therefore $A = a = \frac{f-1}{2}$ and

$$\begin{aligned}(\theta_0 - \theta_1)^2 &= -4(a+1) + 1 \\ &= -2(f+1) + 1 = -\lambda\end{aligned}$$

consistent with the answer to Problem 3.

Page 110, Problem 5. We want to find the general formula for $Ng(\alpha)$ for any prime λ, what we need is the formula from Problem 3 because we need the value of $\theta_0\theta_1$ (to avoid clutter let $r = (-1)^{\frac{\lambda-1}{2}}$)

$$\begin{aligned}(-1)^2 = (\theta_0 + \theta_1)^2 &= \theta_0^2 + \theta_1^2 + 2\theta_0\theta_1 \\ (-1)^{\frac{\lambda-1}{2}}\lambda = (\theta_0 - \theta_1)^2 &= \theta_0^2 + \theta_1^2 - 2\theta_0\theta_1 \\ \rightarrow \frac{1 - r\lambda}{4} &= \theta_0\theta_1\end{aligned}$$

and also

$$\begin{aligned}(-1)^2 = (\theta_0 + \theta_1)^2 &= (\theta_0^2 + \theta_1^2) + 2\theta_0\theta_1 \\ 1 &= (\theta_0^2 + \theta_1^2) + \frac{1 - (-1)^{\frac{\lambda-1}{2}}\lambda}{2} \\ \rightarrow \frac{1 + r\lambda}{2} &= (\theta_0^2 + \theta_1^2)\end{aligned}$$

therefore

$$\begin{aligned} Ng(\alpha) &= (a^2+b^2)\theta_0\theta_1 + ab(\theta_0^2+\theta_1^2) \\ &= (a^2+b^2)\frac{1-r\lambda}{4} + ab\frac{1+r\lambda}{2} \end{aligned}$$

Now as usual let $a+b=u$ and $a-b=v$ first let

$$\begin{aligned} w &= \frac{1-r\lambda}{4} \\ t &= \frac{1+r\lambda}{2} \\ \rightarrow 2w+t &= 1 \\ \rightarrow 2w-t &= -r\lambda = -(-1)^{\frac{\lambda-1}{2}}\lambda \end{aligned}$$

then

$$\begin{aligned} Ng(\alpha) &= \tfrac{1}{4}\left\{(2w+t)u^2 + (2w-t)v^2\right\} \\ &= \tfrac{1}{4}\left\{u^2 - (-1)^{\frac{\lambda-1}{2}}\lambda v^2\right\} \end{aligned}$$

Page 110, Problem 6. Straightforward calculation, $\lambda = 17$, $f = 4$ which means $e = 4$, the smallest primitive root mod 17 is 3, let's first prepare the various σ powers

$$\begin{aligned} \sigma^{1\cdot 4} &\rightarrow \alpha^{3^4} = \alpha^{13} \\ \sigma^{2\cdot 4} &\rightarrow \alpha^{3^8} = \alpha^{16} \\ \sigma^{3\cdot 4} &\rightarrow \alpha^{3^{12}} = \alpha^{4} \end{aligned}$$

therefore the periods are

$$\begin{aligned} \eta_0 &= \alpha + \sigma^e\alpha + \sigma^{2e}\alpha + \sigma^{3e}\alpha \\ &= \alpha + \alpha^{13} + \alpha^{16} + \alpha^4 \\ \sigma\eta_0 = \eta_1 &= \alpha^3 + \alpha^5 + \alpha^{14} + \alpha^{12} \\ \sigma\eta_1 = \eta_2 &= \alpha^9 + \alpha^{15} + \alpha^8 + \alpha^2 \\ \sigma\eta_2 = \eta_3 &= \alpha^{10} + \alpha^{11} + \alpha^7 + \alpha^6 \end{aligned}$$

the multiplication table is

$$\begin{aligned}
\eta_0^2 &= (\alpha^2 + \alpha^9 + \alpha^{15} + \alpha^8) + 2(\alpha^{14} + 1 + \alpha^5 + \alpha^{12} + 1 + \alpha^3) \\
&= \eta_2 + 2(\eta_1 + 2) \\
&= \eta_2 + 2\eta_1 + 4 \\
\eta_0\eta_1 &= 2\eta_0 + \eta_2 + \eta_3 \\
\eta_0\eta_2 &= \eta_0 + \eta_1 + \eta_2 + \eta_3
\end{aligned}$$

we can get $\eta_0\eta_3$ by doing $\sigma^3\eta_1\eta_0 = \eta_{4=0}\eta_3$.

Page 110, Problem 7. We want to know the conditions on a prime p and f that will make the conjugation $\alpha \to \alpha^p$ on the period of length f invariant.

Again, we can always express a prime p as $p \equiv \gamma^j \mod \lambda$, thus the conjugation $\alpha \to \alpha^p$ means $\alpha \to \alpha^{\gamma^j}$ which means $\alpha \to \sigma^j\alpha$ and we want $\sigma^j\eta_i = \eta_{i+j} = \eta_i$. This means that j is a multiple of e. Not sure about conditions on f :)

Page 110, Problem 8. Need to show that the period η_0 is independent of the choice of primitive root. We know that η_0 is the only one that contains α and different primitive roots give the same periods (sans the ordering) therefore η_0 must be the same since it is the only one with α so that's the short story :)

Page 113. Top page, note that what was proven in the previous page is $X^p - X \equiv (X-1)(X-2)\dots(X-p) \mod p$. However, in this page what we have is $g(\alpha)^p - g(\alpha) \equiv (g(\alpha)-1)(g(\alpha)-2)\dots(g(\alpha)-p) \mod p$. So we cannot say that the product on the RHS is a product of p consecutive integers just like when we prove the case for integer X.

But from Page 112 bottom paragraph, the purpose of proving the integer case is to show that the coefficients of $X^p - X - (X-1)(X-2)\dots(X-p)$ are all multiples of p. Of course these are the coefficients once we've multiplied everything out not the coefficients as they are now. Since the cyclotomic integers $g(\alpha)^p - g(\alpha) - (g(\alpha)-1)(g(\alpha)-2)\dots(g(\alpha)-p)$ has the same coefficients they are also $0 \mod p$.

Page 113. Top page, about the proof of the Theorem. Note that in cyclotomic integers the normal prime integers are generally no longer prime cyclotomic. In this proof we have

$$[g(\alpha)-1][g(\alpha)-2]\dots[g(\alpha)-p] \equiv 0 \mod p$$

but it doesn't mean that $p|[g(\alpha)-1]$ or $p|[g(\alpha)-2]$ and so on, it's because p is no longer prime cyclotomic. This is why the proof immediately switches to mod $h(\alpha)$ which is indeed prime cyclotomic.

Another important note, just because $h(\alpha)$ is prime cyclotomic it doesn't mean that it must only divide one $[g(\alpha)-j]$, it can divide two or more. However, if it divides two then

$$g(\alpha)-j \equiv 0 \equiv g(\alpha)-k \mod h(\alpha)$$

which means that $k-j \equiv 0 \mod h(\alpha)$. But this means that $h(\alpha)$ divides a smaller number than p, say $m=|j-k|$. This is impossible because then $Nh(\alpha)|m^{\lambda-1}$ and from $h(\alpha)|p$ we also have $Nh(\alpha)|p^{\lambda-1}$ but since $m<p$ we have $\gcd(m,p)=1$. So only one $[g(\alpha)-j]$ is divisible by $h(\alpha)$.

Page 114, Problem 1. Here we are computing Pascal triangle up to $n=13$ and verifying that the coefficients are multiple of n when n is prime

$$\begin{aligned}
n &= 1 \rightarrow 1\\
n &= 2 \rightarrow 1\ 2\ 1\\
n &= 3 \rightarrow 1\ 3\ 3\ 1\\
n &= 4 \rightarrow 1\ 4\ 6\ 4\ 1\\
n &= 5 \rightarrow 1\ 5\ 10\ 10\ 5\ 1\\
n &= 6 \rightarrow 1\ 6\ 15\ 20\ 15\ 6\ 1\\
n &= 7 \rightarrow 1\ 7\ 21\ 35\ 35\ 21\ 7\ 1\\
n &= 8 \rightarrow 1\ 8\ 28\ 56\ 70\ 56\ 28\ 8\ 1\\
n &= 9 \rightarrow 1\ 9\ 36\ 84\ 126\ 126\ 84\ 36\ 9\ 1\\
n &= 10 \rightarrow 1\ 10\ 45\ 120\ 210\ 252\ 210\ 120\ 45\ 10\ 1\\
n &= 11 \rightarrow 1\ 11\ 55\ 165\ 330\ 462\ 462\ 330\ 165\ 55\ 11\ 1\\
n &= 12 \rightarrow 1\ 12\ 66\ 220\ 495\ 792\ 924\ 792\ 495\ 220\ 66\ 12\ 1\\
n &= 13 \rightarrow 1\ 13\ 78\ 286\ 715\ 1287\ 1716\ 1287\ 715\ 286\ 78\ 13\ 1
\end{aligned}$$

For n prime $2,3,5,7$ are obvious for $n=11$ we have $165=11\cdot 15, 330=11\cdot 30, 462=11\cdot 42$ and for $n=13$ we have $78=13\cdot 6, 286=13\cdot 22, 715=13\cdot 55, 1287=13\cdot 99$, all calculated by hand :)

Page 114, Problem 2. Calculate $X(X-1)(X-2)\dots(X-p+1)$ for $p=3,5,7,11$.

$$\begin{aligned}
p=3 &\to X\dots(X-2) &&= X^3-3X^2+2X\\
p=5 &\to X\dots(X-4) &&= X^5-10X^4+35X^3-50X^2+24X\\
p=7 &\to X\dots(X-6) &&= X^7-21X^6+175X^5-735X^4+1624X^3-1764X^2+720X\\
p=11 &\to X\dots(X-10) &&= X^{11}-55X^{10}+1320X^9-18150X^8+157773X^7-902055X^6+\\
&&&\quad 3416930X^5-8409500X^4+12753576X^3-10628640X^2+3628800X
\end{aligned}$$

to check the (difficult) numbers for $p=7$, $735=7\cdot 105, 1624=7\cdot 232, 1764=7\cdot 252, 720=7\cdot 102+6$, for $p=11$, $1320=11\cdot 120, 18150=11\cdot 1650, 157773=11\cdot 14343, 902055=11\cdot 82005, 3416930=11\cdot 310630, 8409500=11\cdot 764500, 12753576=11\cdot 1159416, 10628640=11\cdot 966240, 3628800=11\cdot 329890+10$. Thus al of them are $\equiv X^p-X \mod p$.

Page 114, Problem 3. We need to verify $\eta^p\equiv\eta \mod p$ in the case of $\lambda=7$, $p=2$ and then for $\lambda=13$ and $p=13$. First, $\lambda=7$ here $\lambda-1=6=2\cdot 3$. So we can either have $e=2, f=3$ or $e=3, f=2$. But $\eta^p\equiv\eta$ only works if η is a period of length f where f is the exponent (or I prefer to call it order) of $p \mod \lambda$.

Here $p=2$ and the order of 2 mod 7 is 3 so $f=3$ and $e=2$, the only primitive roots mod 7 are 3 and 5 and so here we have

$$\begin{aligned}
\eta_0 &= \alpha+\alpha^2+\alpha^4\\
\sigma\eta_0 &= \eta_1=\alpha^3+\alpha^5+\alpha^6
\end{aligned}$$

with $p=2$ we have

$$\begin{aligned}
\eta_0^2 &= \alpha^2+\alpha^4+\alpha+2(\alpha^3+\alpha^5+\alpha^6)\\
&= \theta_0+2\theta_1\\
&\equiv \theta_0 \mod p\\
\eta_1^2 &= \alpha^6+\alpha^3+\alpha^5+2(\alpha+\alpha^2+\alpha^4)\\
&= \eta_1+2\eta_0\\
&\equiv \eta_1 \mod p
\end{aligned}$$

Now, if we choose $e = 3, f = 2$ where f is no longer the exponent of $p \mod \lambda$ then

$$\eta_0 = \alpha + \alpha^6$$
$$\sigma\eta_0 = \eta_1 = \alpha^3 + \alpha^4$$
$$\sigma\eta_1 = \eta_2 = \alpha^2 + \alpha^5$$

again, with $p = 2$ we have

$$\eta_0^2 = \alpha^2 + \alpha^5 + 2 \equiv \eta_2 \mod p$$

which doesn't work :)

Next, is $\lambda = 13$, $p = 3$, the exponent of 3 mod 13 is 3, we also have $\lambda - 1 = 12$, therefore with $f = 3$ (the exponent of $p \mod \lambda$) we must have $e = 4$, the primitive roots mod 13 are 2, 6, 7, 11, let's choose 2

$$\eta_0 = \alpha + \alpha^3 + \alpha^9$$
$$\sigma\eta_0 = \eta_1 = \alpha^2 + \alpha^6 + \alpha^5$$
$$\sigma\eta_1 = \eta_2 = \alpha^4 + \alpha^{12} + \alpha^{10}$$
$$\sigma\eta_2 = \eta_3 = \alpha^8 + \alpha^{11} + \alpha^7$$

with $p = 3$ we have from the formula $(x + y + z)^4 = x^3 + y^3 + z^3 + 3(yz^2 + xz^2 + y^2z + x^2z + xy^2 + x^2y) + 6xyz$

$$\eta_0^3 = \alpha^3 + \alpha^9 + \alpha + 3(\alpha^5 + \alpha^{11} + \alpha^7 + \alpha^6 + \alpha^2 + \alpha^8) + 6 = \eta_0 + 3(\eta_1 + \eta_3) + 6$$
$$\equiv \eta_0 \mod 3$$
$$\eta_1^3 = \alpha^6 + \alpha^5 + \alpha^2 + 3(\alpha^{10} + \alpha^9 + \alpha + \alpha^{12} + \alpha^4 + \alpha^3) + 6 = \eta_1 + 3(\eta_0 + \eta_2) + 6$$
$$\equiv \eta_1 \mod 3$$
$$\eta_2^3 = \alpha^{12} + \alpha^{10} + \alpha^4 + 3(\alpha^7 + \alpha^5 + \alpha^2 + \alpha^{11} + \alpha^8 + \alpha^6) + 6 = \eta_2 + 3(\eta_1 + \eta_3) + 6$$
$$\equiv \eta_2 \mod 3$$
$$\eta_3^3 = \alpha^{11} + \alpha^7 + \alpha^8 + 3(\alpha + \alpha^{10} + \alpha^4 + \alpha^9 + \alpha^3 + \alpha^{12}) + 6 = \eta_3 + 3(\eta_0 + \eta_2) + 6$$
$$\equiv \eta_3 \mod 3$$

Page 114, Problem 4. Show that for a prime λ, any prime factor of $k^{\lambda-1} + k^{\lambda-2} + \cdots + 1$ are either 0 or 1 $\mod \lambda$. The main thing here is that "any prime factor of" not just that the whole sum is $0, 1 \mod \lambda$ even though it is.

If $k = 1$ then the sum is exactly λ and we have $0 \mod \lambda$, if $k \neq 1$ then from geometric series we have the sum to be $\frac{k^\lambda - 1}{k-1} \equiv \frac{k-1}{k-1} \equiv 1 \mod \lambda$ (where we have used Fermat's Little Theorem $k^\lambda \equiv k \mod \lambda$).

But the above geometric formula also applies mod any prime factor p of the sum (as long as $k \neq 1$), *i.e.* $k^{\lambda-1} + k^{\lambda-2} + \cdots + 1 = \frac{k^\lambda - 1}{k-1} \equiv 0 \mod p$, it is $0 \mod p$ because p is a prime factor of the sum.

This means that $k^\lambda \equiv 1 \mod p$, therefore it's either $k = 1$ (the only element with order one is $k = 1$) or the order of k mod p is λ (because λ is prime otherwise the order can be any factor of λ). But $k = 1$ is already covered above and we have explicitly assumed that $k \neq 1$ in this case so that we were able to use the geometric series formula so the order of k is λ. Then Fermat's Little Theorem tells us that $\lambda | p - 1$ and we immediately have $p \equiv 1 \mod \lambda$.

Page 114, Problem 5. Here we have $\lambda = 5$ and $p = 19$, here we want to show that p has a prime factor then the u_i in $\eta_i \equiv u_i \mod p$ obeys $u^2 + u - 1 \equiv 0 \mod p$.

It is simple enough since $\lambda - 2 = 4 = 2 \cdot 2$ thus $e = 2, f = 2$. Note that if we force $e = 1, f = 4$ then $\eta_0 = -1$ (because it's just the sum of all powers of α) and $(-1)^2 - 1 - 1 \not\equiv 0 \mod 19$. Likewise with $e = 4, f = 1$. This is actually obvious since quadratic u must have only two solutions and if $e = 4$ we have four η.

So with $e = 2, f = 2$ we have (choosing 2 as the primitive root mod 5)

$$\eta_0 = \alpha + \alpha^4$$
$$\eta_1 = \alpha^2 + \alpha^3$$

Therefore, the multiplication table is

$$\eta_0^2 = \eta_1 + 2 = -1 - \eta_0 + 2$$
$$\rightarrow 0 = \eta_0^2 + \eta_0 - 1$$

since $\eta_0 + \eta_1 = -1$. Applying $\sigma \eta_0^2 = \eta_1^2 = 1 - \eta_1$ So if $\eta_i \equiv u_i \mod p$ therefore $u_i^2 + u_i - 1 \equiv 0 \mod 19$, solving it we get $u_i(u_i + 1) \equiv 1 \mod 19$. The solution is $u_i = 4$ and $u_i = -5$ and these are the only two solutions since we only have two η.

Next we are asked to show that $\eta_0 - u$ divides p, note that $\eta_0 \equiv u \ (p)$ means that $p | \eta_0 - u$ and not the other around. What we need to show is the other way around.

For one thing the norm $N(\eta_0 - 4) = N(\eta_0 + 5) = 19^2$. This means that (let $f(\alpha) = \eta_0 - 4$), arranging things judiciously :)

$$\begin{aligned} Nf(\alpha) = 19 \cdot 19 &= \{f(\alpha)f(\alpha^2)\} \cdot \{f(\alpha^3)f(\alpha^3)\} \\ &= \{19\} \cdot \{19\} \end{aligned}$$

where $f(\alpha) = f(\alpha^4) = \eta_0 - 4$ and $f(\alpha^2) = f(\alpha^3) = \eta_1 - 4$. And the factorization is therefore $(\eta_0 - 4)(\eta_1 - 4) = 19$.

I was initially tempted to arrange things by complex conjugation $(f(\alpha)f(\alpha^4)) \cdot (f(\alpha^2)f(\alpha^3))$ but it didn't work out well because each term, even though positive real numbers, was not an integer.

We know need to show that these factors of 19, $\eta_0 - 4$ and $\eta_1 - 4$, are irreducible. Well if they are reducible then

$$\begin{aligned} h(\alpha)g(\alpha) &= \eta_0 - 4 \\ Nh(\alpha)Ng(\alpha) &= 19^2 \end{aligned}$$

which means that $Nh(\alpha) = Ng(\alpha) = 19$ for η_0 to be reducible but just like the proof on Page 113, $Nh(\alpha) = h(1)^{\lambda-1} \equiv 0, 1 \mod \alpha - 1$. From Page 93 we know that $\alpha - 1$ is prime, its norm is λ therefore $Nh(\alpha) = h(1)^{\lambda-1} \equiv 0, 1 \mod \lambda$.

In this case $Nh(\alpha) = 19$ so it can't be $0 \mod \lambda$. Therefore it must be $1 \mod \lambda = 5$ but 19 is not $1 \mod 19$ thus contrary to our assumption, $\eta_0 - 4$ is irreducible. The same arguments goes for $\eta_1 - 4$. There are also other factorizations like $(\eta_0 + 5)(\eta_1 + 5) = 19$ and by the same argument above each factor is also irreducible.

Page 114, Problem 6. We are now factoring 3 into its irreducible factors like in Problem 5 but here $\lambda = 13$, $\lambda - 1 = 12$. To make things simple let's try with $e = 2, f = 6$ so that we only have two periods (choosing 2 as the primitive root)

$$\begin{aligned} \eta_0 &= \alpha + \alpha^4 + \alpha^3 + \alpha^{12} + \alpha^9 + \alpha^{10} \\ \eta_1 &= \alpha^2 + \alpha^8 + \alpha^6 + \alpha^{11} + \alpha^5 + \alpha^7 \end{aligned}$$

the multiplication table is

$$\begin{aligned} \eta_0^2 &= \eta_1 + 2(\eta_1 + \eta_0 + 3) \\ &= 3 - \eta_0 \end{aligned}$$

this means that if $\eta_0 \equiv u \mod p$ then $u^2 + u - 3 \equiv u(u+1) \equiv 0 \mod 3$ meaning $u = 2$ or $u = -3$ (we can also set $u = 0$).

As in Problem 5 the factorization is $3 = (\eta_0 - 2)(\eta_1 - 2) = (\eta_0 + 3)(\eta_1 + 3)$, if we use $\eta_0 \equiv 0$ we get $-3 = \eta_0\eta_1 \rightarrow 3 = -\eta_0\eta_1$ which is another factorization.

Page 114, Problem 7. We want to show that if f is an exponent of p mod λ then if $Ng(\alpha) = p^f$ then $g(\alpha)$ is irreducible.

This is similar to Problem 5 and also very similar to the proof on Page 13. Assume that $g(\alpha)$ is reducible then

$$f(\alpha)h(\alpha) = g(\alpha)$$
$$Nf(\alpha)Nh(\alpha) = p^f$$

since $g(\alpha)$ is assumed to be reducible then $Nf(\alpha) = p^a$ where $0 < a < f$. Following the logic of the proof on page 113, $Nf(\alpha) \equiv f(1)^{\lambda-1} \equiv 0, 1 \mod \alpha - 1 \equiv 0, 1 \mod \lambda$ since from Page 93 we know that $\alpha - 1$ is prime and its norm is λ (so $\alpha - 1 | \lambda$) but since $Ng(\alpha) = p^a$ it must be $1 \mod \lambda$. This means that $p^a \equiv 1 \mod \lambda$ which means that a must be a multiple of f contrary to our assumption that $0 < a < f$. Therefore, $g(\alpha)$ is irreducible.

Page 114. Summary of Section 4.7

The theme in Edwards' books (at least the one I keep seeing) is that we don't need to rely on formulas all the time. We just need to know what needs to be done and find ways to do it. For example, the formula to find a prime factor of a prime integer is to construct $g(\alpha) = a + b\eta_0 + c\eta_1 + \ldots$ such that $Ng(\alpha) = p^f$. But that is not what he did for the first part on this section. Instead, by calculating the norm we see that simple trial and errors will give us the solution.

This also explains how many conjugates we need to test if a candidate works as a prime factor. We know that $Ng(\alpha) = p^f$ and there are ef terms in $Ng(\alpha)$ but what we want is a prime factor of p therefore a group of e conjugates must form one p, thus once we get a candidate we just need to multiply e conjugates to see if their product contains p.

The next comment I have is that when factoring prime integers, say $e = 2$, so we only have two periods θ_0 and θ_1, once we find that say $(\theta_0 - 3)$ is a factor then we immediately

know that the factorization must be $(\theta_0 - 3)(\theta_1 - 3)$. This is because we know that the norm is $Ng(\alpha) = p^f$ but the norm is also of the form $[(a + b\theta_0)(a + b\theta_1)]^f$.

Finally, this is actually the same method as discussed previously on Section 4.4 for $p \equiv 1 \mod \lambda$. In that case the periods are all of length 1 because that's the exponent of p. But periods of length one is just α^j and the $\eta_i \equiv u_i$ just means $\alpha \equiv k$.

Page 116. Top Page. "the desired factor of 59 can be found by dividing by two suitable factors of 11". Why two suitable factors? Recall that 11 has four prime factors and what we have is

$$N(25 - \theta_0) = (25 - \theta_0)(25 - \theta_1)(25 - \theta_0)(25 - \theta_1) = 11^2 \cdot 59^2$$

There are four factors in the LHS and there are two copies of 11, each carrying four factors, so we have 8 factors we need to spread into the four in the LHS, therefore each factor in the LHS should have 2 suitable factors of 11.

Page 116. Top Page, near the end of first paragraph, "It is also divisible by $\alpha^4 + 2$ because the conjugation $\alpha \to \alpha^4$ leaves θ_0 and θ_1 invariant." Earlier we saw that $\alpha + 2|25 - \theta_0$, conjugating $(\alpha \to \alpha^4)$ we get $\alpha^4 + 2|25 - \theta_0$.

Page 116. Top Page, calculation after first paragraph, it is refreshing to see that we are not using the normal algorithm $f(\alpha)g(\alpha) = h(\alpha) \to g(\alpha) = \frac{h(\alpha)f(\alpha^2)f(\alpha^3)...f(\alpha^{\lambda-1})}{Nf(\alpha)}$. Here, the thing we need to remember is that $(a + b\theta_0)(a + b\theta_1)$ gives you an integer. So we can use this information to do division like in this case.

Page 116. Mid(ish) Page, factorization of 79, it is interesting that even though the congruence is $a + 29b - 30c \equiv 0 \mod 79$ we did not choose the simplest solution $a = 29, b = -1, c = 0$ like usual. Maybe he already knew that this solution $\to (29 - \theta_0)$ results in $(29 - \theta_0)(29 - \theta_1) = 11 \cdot 29$. The other simple solution $a = 30, b = 0, c = 1$ results in $(30 + \theta_0)(30 + \theta_1) = 11 \cdot 79$ as well. We can of course divide it by the suitable factors of 11, two of them since there are four prime factors of 11 and there are two terms in the LHS. Let's try it.

A prime factor of 11 is $\alpha + 2$, like before $\theta_0 \equiv 3 \mod \alpha + 2$ and $\theta_1 \equiv -4$, $29 - 3 \not\equiv 0 \mod 11$ but $30 + 3 \equiv 0 \mod 11$ so let's just divide our second solution. We need to find another factor of 11 to divide $30 + \theta_0$ but as mentioned in the book, conjugating $\alpha \to \alpha^4$

doesn't change $\theta_{0,1}$ so the two factors are $\alpha+2$ and α^4+2

$$\frac{30+\theta_0}{(\alpha+2)(\alpha^4+2)} = \frac{(30+\theta_0)(5+2\theta_1)}{(5+2\theta_0)(5+2\theta_1)}$$
$$= \frac{150+60\theta_1+5\theta_0-2}{11} = \frac{143+55\theta_1}{11} = 13+5\theta_1$$

which is another factor of 79 while we're at it let's divide $29-\theta_0$ as well, here the prime factor of 11 that works must be α^2 since α and therefore α^4 don't work

$$\frac{29-\theta_0}{(\alpha^2+2)(\alpha^3+2)} = \frac{(29-\theta_0)(5+2\theta_0)}{(5+2\theta_1)(5+2\theta_0)}$$
$$= \frac{145+58\theta_0-5\theta_0-2(1-\theta_0)}{11} = \frac{143+55\theta_0}{11} = 13+5\theta_0$$

which is just the conjugate of the previous solution.

Page 118. Second Paragraph, and other places also it says something like "Therefore $a+b\eta_0+c\eta_1+d\eta_2$ is divisible by a prime divisor of 13 only if it or one of its conjugates satisfies $a-3b-5c-6d \equiv 0 \mod 13$'. Why "one of its conjugates"? because the values of u_i's are the cyclic permutations of $(-3,-5,-6)$, when you permute you get the conjugate because you're exchanging the η_i's.

Page 121, Problem 1. $\lambda=7$, $\eta_2-\eta_1+1$ divides η_0+3, we need to show that the quotient is a unit. Here $f=2$ and $e=3$ and we know it divides η_0+3 because mod $\eta_2-\eta_1+1$ we have $\eta_0 \equiv -3$.

The norm $N(\eta_0+3)$ must be a product of cyclic permutations of the η's because a conjugation of one η gives you another η and since there are only 3 η's we must have $\{(\eta_0+3)(\eta_1+3)(\eta_2+3)\}^2$

$$(\eta_0+3)(\eta_1+3) = \eta_0\eta_1+3(\eta_0+\eta_1)+9$$
$$= (\eta_1+\eta_2)-3(1+\eta_2)+9 = (\eta_1-2\eta_2)+6$$
$$\rightarrow (\eta_0+3)(\eta_1+3)(\eta_2+3) = \eta_1\eta_2-2\eta_2^2+6\eta_2+3\eta_1-6\eta_2+18$$
$$= (\eta_2+\eta_0)-2(2+\eta_1)+3\eta_1+18$$
$$= (\eta_0+\eta_1+\eta_2)+14$$
$$= 13$$

Therefore $N(\eta_0+3)=13^2$. This means that the quotient is indeed a unit. We now need to find this unit and its inverse (the real calculation is too long to type, I'll just put the

final result here, it took me three tries to get it right)

$$\begin{aligned}\frac{\eta_0+3}{\eta_2-\eta_1+1} &= \frac{(\eta_0+3)(\eta_0-\eta_2+1)(\eta_0-\eta_1-1)}{(\eta_2-\eta_1+1)(\eta_0-\eta_2+1)(\eta_0-\eta_1-1)} \\ &= \frac{3+3\eta_0-10\eta_1+3\eta_2}{13} \\ &= \frac{13+13\eta_0+13\eta_2}{13} \\ &= 1+\eta_0+\eta_2\end{aligned}$$

As a check $N(1+\eta_0+\eta_2)=1$, the inverse of this unit is $f(\alpha^2)f(\alpha^3)f(\alpha^4)f(\alpha^5)f(\alpha^6) = 1+\eta_2$ where $f(\alpha)=1+\eta_0+\eta_2$.

Page 121, Problem 2. Derive last line of Table 4.7.5, a factorization of 97 when $\lambda=7$. First, 97 has an exponent $f=2$ so we are using periods with length 2 given on Page 117. The relationships among the u_i's are given on Page 118, we need to find $u_0^3+u_0^2-2u_0-1\equiv 0 \mod 97$. Trying out different u_0's (this one really tries your patience) you get $u_0=25$. Therefore $u_2\equiv u_0^2-2\equiv 41 \mod 97$, $u_1\equiv -1-u_0-u_2\equiv 30 \mod 97$.

So the u_i's are cyclic permutations of $(25,41,30)$ and $a+b\eta_0+c\eta_1+d\eta_2$ is divisible by prime divisor of 97 if it (or its conjugates) satisfies $a+25b+41c+30d\equiv 0 \mod 97$. Let's try out the simple solutions, from the answer in the Table, it seems like we need to do some division.

The simple ones give not so good answers the best one is η_0-30 giving $(\eta_0-30)(\eta_1-30)(\eta_2-30)=7\cdot 41\cdot 97$ and we need to do division, seven is obviously the norm of $\alpha-1$.

The not so simple choices like $(a=16)+25(b=1)+41(c=-1)$ is quite tricky, I initially assigned $\eta_0\equiv 25$ and $\eta_1\equiv 41$ and it didn't work, what works is $\eta_0\equiv 41$ and $\eta_1\equiv 25$. Here we get $41\cdot 97$ from $16+\eta_1-\eta_0$.

Trying another not so simple one I got the answer immediately $-5+\eta_0-\eta_2$, $\eta_0\equiv 30, \eta_2\equiv 25$ with

$$(-5+\eta_0-\eta_2)(-5+\eta_1-\eta_0)(-5+\eta_2-\eta_1)=-97$$

A different result from the book's. However, this is actually a good exercise because the table gives a different assignment $\eta_0\equiv 25$ and $\eta_2\equiv 41$ due to this we can't divide $(-5+\eta_0-\eta_2)$ by $4\eta_0-3$.

So the lesson here is that once the assignment $\eta_i \equiv u_i \mod p$ is made the prime factor is also determined, different u_i will generate different prime factors.

To get the result in the book we need $5 + \eta_0 - \eta_1$ with

$$(5 + \eta_0 - \eta_1)(5 + \eta_1 - \eta_2)(5 + \eta_2 - \eta_0) = 97$$

to get the result in the table we just need to multiply this by a unit $-1 + \eta_0$:)

Page 121, Problem 3. Here we calculate the prime p under 100 that also has exponent 3 mod $\lambda = 13$. This prime is 61. We now need to find the factors of 61, again we need to solve $u_0^4 + u_0^3 + 2u_0^2 - 4u_0 + 3 \equiv 0 \mod 61$. The hint says that $u = 10$ solves it. Let's try it $10000 + 1000 + 200 - 40 + 3 = 1079 = 61 \cdot 183$ and so it works :)

So we have $3u_2 \equiv 3 - 2u_0 - u_0^3 \equiv 27 \mod 61$ and $u_1 \equiv u_0^2 - 2u_2 \equiv 46 \mod 61$ and $u_3 \equiv -1 - u_0 - u_1 - u_2 \equiv 38 \mod 61$, so the equation is $a + 10b + 46c + 27d + 38e \equiv 0 \mod 61$. So now we get to trial and error.

Since $f = 3$ then $e = 4$, the smallest primitive root mod 13 is 2 so

$$\eta_0 = \alpha + \alpha^3 + \alpha^9$$
$$\eta_1 = \alpha^2 + \alpha^5 + \alpha^6$$
$$\eta_2 = \alpha^4 + \alpha^{10} + \alpha^{12}$$
$$\eta_3 = \alpha^7 + \alpha^8 + \alpha^{11}$$

Trial and error might take a while so I wrote a Python script :)

```
def generateEtas(L, f):
    e = (L-1)/f

    # create eta's
    g = primRoots(L)[0]

    eta = [[0] * L for i in xrange(e)]

    for i in xrange(e):
        for j in xrange(f):
            eta[i][pow(g,j*e+i,L)] = 1

        print u'\u03B7%d =' % (i), eta[i]

    return eta

def findEtaNz(eta):

    e = len(eta)
```

```
    L = len(eta[0])

    nz = [0] * e

    for i in xrange(e):
        for j in xrange(L):
            if eta[i][j] != 0:
                nz[i] = j
                break

    return nz

# function to print sums of eta's
def printSumEtaRaw(res, nz):
    e = len(nz)
    m = 0
    for j in xrange(e):
        if res[nz[j]] != 0:
            if res[nz[j]] < 0:
                print '-'
            elif m > 0:
                print '+',
            print u'%d*\u03B7%d' % (abs(res[nz[j]]), j),
            m += 1


    if res[0] < 0:
        print '-', abs(res[0])
    elif res[0] > 0:
        print '+', abs(res[0])
    else:
        print

# print out multiplication table for periods
def multTablePeriods(L, f):

    e = (L-1)/f
    eta = generateEtas(L, f)

    # first get non zero index of each eta
    nz = findEtaNz(eta)

    # now build the multiplication table if there are e periods
    # then there are e main terms plus e(e-1)/2 cross terms

    for i in xrange(e):
        res = multCyc(eta[i], eta[i])

        print u'\u03B7%d^2 = ' % (i),
        printSumEtaRaw(res, nz)


    # now check for cross terms
    for i in xrange(e-1):
        for j in xrange(1,e):
            res = multCyc(eta[i], eta[j])
```

```
            print u'\u03B7%d*\u03B7%d = ' % (i, j),
            printSumEtaRaw(res, nz)


# find u_i corresponding to eta_i
def FindU(L, p, e):

    if L == 5:
        for i in xrange(1,1000):
            if ((i*(i+1)) % p) == 1:
                u = [i, -(i+1)]
                break

    elif L == 13:
        u = [0] * e
        for i in xrange(100):
            if e == 4:
                if ((pow(i,4,p) + pow(i,3,p) + 2*pow(i,2,p) - 4*i + 3) % p) == 0:
                    u[0] = i
                    break
                if ((pow(-i,4,p) + pow(-i,3,p) + 2*pow(-i,2,p) - 4*(-i) + 3) % p) == 0:
                    u[0] = -i
                    break
            elif e == 3:
                if ((pow(i,3,p) + pow(i,2,p) - 4*i + 1) % p) == 0:
                    u[0] = i
                    break
                if ((pow(-i,3,p) + pow(-i,2,p) - 4*(-i) + 1) % p) == 0:
                    u[0] = -i
                    break
            elif e == 2:
                if ((pow(i,2,p) + i -3) % p) == 0:
                    u[0] = i
                    break
                if ((pow(-i,2,p) + (-i) -3) % p) == 0:
                    u[0] = -i
                    break
        print u[0]
        if e == 4:
            # find inverse of 3 mod p
            for i in xrange(1,p):
                if (i*3) % p == 1:
                    i3 = i
                    break
            else:
                i3 = 0

            u[2] = (i3 * (3 - 2*u[0] - pow(u[0],3,p))) % p
            u[1] = (pow(u[0],2,p) - 2*u[2]) % p
            u[3] = (-1 -u[0] - u[1] - u[2] ) % p
        elif e == 3:
            u[2] = (pow(u[0],2,p) + u[0] - 3) % p
            u[1] = (-1 - u[0] - u[2]) % p
        elif e == 2:
            u[1] = (-1 - u[0]) % p

    return u
```

```
def printEtaFactor(res):
    ln = len(res)

    for j in xrange(ln-1):
        m = 0

        print '(',
        for i in xrange(1,ln):
            if res[i] != 0:
                if res[i] < 0:
                    print '-',
                elif m > 0:
                    print '+',
                print u'%d*\u03B7%d' % (abs(res[i]), ((i-1)+j) % (ln-1)),
                m += 1

        if res[0] < 0:
            print '-', abs(res[0]),
        elif res[0] > 0:
            print '+', abs(res[0]),
        print ')',

    print


# find factors of prime numbers
def Page121Problem3and5(L, p):

    # first find order of p mod L
    for i in xrange(1,L):
        if pow(p,i,L) == 1:
            f = i
            break

    print 'f', f
    e = (L-1)/f

    # create eta's

    eta = generateEtas(L, f)

    u = FindU(L,p,e)

    for i in xrange(e):
        print 'u%d: %d,' % (i, u[i]),
    print

    g = primRoots(L)[0]
    min_e = searchMinE(L)

    import itertools
    t = [i for i in range(1,e+1)]

    for y in xrange(1,e + 1):

        l = itertools.combinations(t, y)

        for i in l:
```

```
# create a bitmap for the plus minus
for k in range(0,2**y):
    res = [0] * (e+1)
    for j in range(y):
        b = pow(-1,(k >> j) & 0x01)
        res[i[j]] = b*1
        res[0] -= b*u[i[j]-1]

    cd = [0] * L
    for j in xrange(1,len(res)):
        et = [res[j] * z for z in eta[j-1]]
        cd = addCyc(cd, et)
    cd[0] = res[0]
    N = cycNormFast(f=cd, g=g, e=min_e)

    # we actually don't need to calculate the norm
    # we can straight away do the verification below
    # but this serves as a double-check

    if N == pow(p,f):
        print N, res

        # check result to see if we need a minus sign
        tmp = [0] * L
        tmp[0] = res[0]
        for j in xrange(1,e + 1):
            et = [res[j] * w for w in eta[j-1]]
            tmp = addCyc(tmp, et)

        tot = [w for w in tmp]
        for j in xrange(1,e):
            tmp = cycShift(tmp, g)
            tot = multCyc(tot, tmp)

        # check if all elements from index 1 to L-1 are the same
        for j in xrange(2,L):
            if tot[j] != tot[j-1]:
                print 'Tot is not right'
                break
        else:
            print tot[0] - tot[1], '=',

        # this is just cosmetics but it's worth it
        printEtaFactor(res)
```

The weakness of this script is I always assign η_i to $\pm u_i$ there's no cyclic permutation I can add that in the future. For $\lambda = 13$ and $p = 61$ the result is

$$61 = (1 + \eta_0 + \eta_2 - \eta_3)(1 + \eta_1 + \eta_3 - \eta_0)(1 + \eta_2 + \eta_0 - \eta_1)(1 + \eta_3 + \eta_1 - \eta_2)$$

Page 121, Problem 4. We need to calculate the next prime with exponent 2 mod $\lambda = 5$. The next prime is 109. We need to solve $u^2 + u - 1 \equiv 0 \mod 109$ the solutions are

$10, -11$.So what we have is $a + 10b - 11c \equiv 0 \mod 109$ but again we can use the script above to immediately get the solution

$$109 = (\eta_0 - 10)(\eta_1 - 10)$$

Page 121, Problem 5, The only possible exponents of $\lambda = 13$ are $1, 2, 3, 4, 6, 12$, exponent 1 and 12 are not of interest since exponent 1 was dealt with in earlier Sections and exponent 12 means that the prime is its own prime factor. The exponents of the prime less than 100 are, $f = 1 \rightarrow 53, 79$, $f = 3 \rightarrow 3, 29, 61$, $f = 4 \rightarrow 5, 31, 47, 73, 83$, $f = 6 \rightarrow 17, 23, 43$, the rest of the primes have exponent of 12 they are $2, 7, 11, 19, 37, 41, 59, 67, 71, 89, 97$.

So we need to factorize the first prime with exponent bigger than 2, they are $f = 3 \rightarrow 3$, $f = 4 \rightarrow 5$ and $f = 6 \rightarrow 17$.

For $f = 4, e = 3$ the multiplication table is

$$\eta_0^2 = \eta_1 + 2\eta_2 + 4$$
$$\eta_0\eta_1 = \eta_0 + 2\eta_1 + \eta_2$$
$$\eta_0\eta_2 = 2\eta_0 + \eta_1 + \eta_2$$

The equations obeyed by u are

$$u_0^2 \equiv u_1 + 2u_2 + 4$$
$$u_0u_1 \equiv u_0 + 2u_1 + u_2$$
$$u_0u_2 \equiv 2u_0 + u_1 + u_2$$

Then

$$\begin{aligned} u_0^3 &\equiv u_0u_1 + 2u_0u_2 + 4u_0 \\ &\equiv u_0 + 2u_1 + u_2 + 2(2u_0 + u_1 + u_2) + 4u_0 \\ &\equiv 9u_0 + 4u_1 + 3u_2 \end{aligned}$$

adding u_0^2 to both sides

$$\begin{aligned} u_0^3 + u_0^2 &\equiv 9u_0 + 5u_1 + 5u_2 + 4 \\ &\equiv 9u_0 - 5 - 5u_0 + 4 \\ 0 &\equiv u_0^3 + u_0^2 - 4u_0 + 1 \end{aligned}$$

To get the rest

$$u_0^2 \equiv (-1 - u_0 - u_2) + 2u_2 + 4$$
$$u_2 \equiv u_0^2 + u_0 - 3$$

For $f = 6, e = 2$ the multiplication table is

$$\eta_0^2 = 2\eta_0 + 3\eta_1 + 6$$
$$\eta_0\eta_1 = 3\eta_0 + 3\eta_1$$

But of course $\eta_1 = -1 - \eta_0$ so

$$u_0^2 \equiv 2u_0 + 3(-1 - u_0) + 6$$
$$0 \equiv u_0^2 + u_0 - 3$$

I then fed these relationships among the u's to the Python script above which resulted in

$$3 = \eta_0\eta_1\eta_2\eta_3$$
$$5 = (\eta_0 + 1)(\eta_1 + 1)(\eta_2 + 1)$$
$$17 = (\eta_0 - 4)(\eta_1 - 4)$$

with the understanding that the η_0 for 3 is different from the one for 5 and 17 since the period lengths are all different for each of the primes.

Page 122. Top page, "$P(X)$ depends only on which powers of α lie in the same period η_0 ... Therefore, in the examples, the coefficients ... must all be independent of the choice γ." I'm not convinced by this and I have a counter example. I noticed that this might not be true when doing Problem 3.

The problem is that η_0^2 is also a polynomial that depends only on powers of α that lie only in η_0 but we all know that η_0^2 involves other η's. This is because a product of $\alpha^j \cdot \alpha^k$ both in η_0 can result in α^l which is in another η.

Page 122. Top page, we can see that the coefficients of $P(X)$ are all made up of periods because from its definition $P(X) = \prod_{i=1}^{f}(X - \sigma^{ei}\alpha)$ which means that $P(X)$ is invariant under σ^e and according to Proposition 110.0 (or if you think about it enough) $P(X)$ can only be made of periods and constants.

Page 124. Last major paragraph of the proof, first "$\psi(\alpha)\alpha, \psi(\alpha)\alpha^2, \ldots, \psi(\alpha)\alpha^\lambda = \psi(\alpha)$ are all nonzero mod $h(\alpha)$ (because $h(\alpha)$ is prime)". This is because otherwise $\psi(\alpha)\alpha^j \equiv 0 \mod h(\alpha)$ but since $h(\alpha)$ is prime it must divide either $\psi(\alpha)$ or α^j but both are not divisible by $h(\alpha)$.

Second, "because $\psi(\alpha)\alpha^j \equiv \psi(\alpha)\alpha^k$ would imply $\alpha^j \equiv \alpha^k$". This is because otherwise

$$\psi(\alpha)\alpha^j \equiv \psi(\alpha)\alpha^k \rightarrow \psi(\alpha)\alpha^j - \psi(\alpha)\alpha^k \equiv 0 \mod h(\alpha)$$

which means that $h(\alpha)$ either divides $\psi(\alpha)$ or $\alpha^j - \alpha^k$.

Lastly, "$\psi(\alpha)\alpha^j \equiv \alpha^i$ would imply $\psi(\alpha) \equiv \alpha^k$", again, otherwise $\psi(\alpha)\alpha^j - \alpha^i \equiv 0$ mod $h(\alpha)$ and since $h(\alpha)$ is prime it must either divide $\psi(\alpha)$ or $\psi(\alpha) - \alpha^{i-j}$.

Page 124. Last major paragraph of the proof, when counting nonzero incongruent cyclotomic integers the funny thing here is that going from $\alpha, \alpha^2, \ldots, \alpha^\lambda = 1$ to the next nonzero incongruent ones we just multiply them $\alpha^j\psi(\alpha)$ instead of $\alpha^j + \alpha^k\psi(\alpha)$ which is done in Problem 4 to count that there are p^n elements in the group S. This is because we are only counting the nonzero ones while Problem 4 includes zero. See Problem 4 for more detail.

Page 124, Problem 1. Here we want to calculate $P(X)$ of Page 122 for different λ and f.

$$\begin{aligned}
\lambda &= 5 \quad f = 2 \rightarrow 1 - \eta_0 X + X^2 \\
\lambda &= 7 \quad f = 2 \rightarrow 1 - \eta_0 X + X^2 \\
\lambda &= 11 \quad f = 5 \rightarrow -1 + 157\eta_1 X - 157\eta_0 X^2 + X^5 \\
\lambda &= 13 \quad f = 3 \rightarrow -1 + \eta_2 X - \eta_0 X^2 + X^3 \\
\lambda &= 31 \quad f = 5 \rightarrow e - 1 + \eta_3 X - (\eta_4 - \eta_5)X^2 + (\eta_1 + \eta_2)X^3 - \eta_0 X^4 + X^5
\end{aligned}$$

again this was all done using a Python script

```
def Page124Problem1(L, f):

    e = (L-1)/f
    g = primRoots(L)[0]

    eta = generateEtas(L, f)
    nz = findEtaNz(eta)

    # build P(X) here X = 13
```

```
P = [0] * L
P[0] = 13
P[1] = -1

p = [i for i in P]

for i in xrange(1,f):
    tmp = cycShift(p, pow(g,i*e,L))
    print tmp
    P = multCyc(P, tmp)

print P

# search for power of 13

res = [[0] * L for i in xrange(f)]

# first try to calculate the constant term
c = P[0] - pow(13, f)
P[0] -= c

for i in xrange(f,0,-1):
    t = pow(13,i)
    for j in xrange(L):
        if P[j] != 0:
            if P[j] % t == 0:
                res[i-1][j] = P[j] / t
                P[j] = 0

P[0] += c
res.insert(0,P)

print res

print '(%+d)' % res[0][0],

# now see which eta is which
for i in xrange(1,f):
    print '(',
    for j in xrange(e):
        if res[i][nz[j]] != 0:
            print u'%+d*\u03B7%d' % (res[i][nz[j]],j),
    print ')*X^%d' % i,

if res[f][0] != 1:
    print 'res[f][0] not one, something wrong'

for j in xrange(1,L):
    if res[f][j] != 0:
        print 'res[f] is not right'
        break

print '(%+d)*X^%d' % (res[f][0], f)
```

Page 124, Problem 2. If you multiply all of them $(\alpha^3+3\alpha^2+12\alpha-1)(\alpha^3-14\alpha^2+$

$5\alpha - 1)(\alpha^3 - 12\alpha^2 - 3\alpha - 1)(\alpha^3 - 5\alpha^2 + 14\alpha - 1)$ you get

$$\alpha^{12} - 28\alpha^{11} + 233\alpha^{10} - 666\alpha^9 + 2611\alpha^8 - 8090\alpha^7 + 30103\alpha^6 - 8090\alpha^5 + 2611\alpha^4 - 666\alpha^3 + 233\alpha^2 - 28\alpha + 1$$

But $-28 \equiv 233 \equiv -666 \equiv 2611 \equiv -8090 \equiv 30103 \equiv 1 \mod 29$, thus the whole thing is $\equiv \alpha^{12} + \alpha^{11} + \alpha^{10} + \cdots + 1 \equiv 0 \mod 29$. This is actually a cool technique, factoring a polynomial mod p using cyclotomic integers. We finally learn an application of cyclotomic integers :)

Page 125, Problem 3. So first thing to do is to get $P(X)$ of page 122. To choose e and f we set f to be the exponent of prime p mod λ. Once we get $P(X)$ we need the congruences $\eta_i \equiv u_i$, these we get from factoring p using the technique of Section 4.7.

First one we to to factorize is $X^4+X^3+X^2+X+1$ mod 19, mod 59 and mod 41. Here $\lambda = 5$, the corresponding exponents f are $2, 2, 1$ respectively. The $P(X)$ is $X^2 - \eta_0 X + 1$ and $X - \alpha$ respectively.

For $p = 19$, we have $\eta_0 \equiv 4, \eta_1 \equiv -5$. So the factors are $(X^2-4X+1)(X^2+5X+1) = X^4 + X^3 - 18X^2 + X + 1$ and $-18 \equiv 1 \mod 19$ so it works.

For $p = 59$, $\eta_0 \equiv 25, \eta_1 \equiv -26$. So the factors are $(X^2 - 25X + 1)(X^2 + 26X + 1) = X^4 + X^3 - 648X^2 + X + 1$ and $-648 \equiv 1 \mod 59$ so it works.

For $p = 41$ this is different since the exponent is 1, *i.e.* $41 \equiv 1 \mod 5$. Therefore $P(X) = X - \alpha$ and if we substitute $X = \alpha$ we just get $0 = 0$. But we should not just follow a formula blindly. The crux of the method in Problem 2 is that we want to multiply f number of cyclotomic integers where each of them contains a different conjugation of a prime factor of p.

In the case of $p = 41$, from Page 98 we know that the prime factor of p divides $\alpha + 4 \to \alpha \equiv -4$, therefore $(\alpha - (-4))$ contains one conjugate of the prime factor of p, another conjugate would be contained in $\alpha^2 \equiv -4$ here $\lambda = 5, \alpha^5 = 1$ so $(\alpha^2)^3 \equiv \alpha \equiv (-4)^3$, yet another conjugate is in $\alpha^3 \equiv -4 \to (\alpha^3)^2 \equiv \alpha \equiv (-4)^2$ and the last one is in $\alpha^4 \equiv -4 \to (\alpha^4)^4 \equiv \alpha \equiv (-4)^4$ so the factorization is

$$(\alpha - (-4))(\alpha - (-4)^3)(\alpha - (-4)^2)(\alpha - (-4)^4) = \alpha^4 - 204\alpha^3 - 14144\alpha^2 + 208896\alpha + 1048576$$

and $-204 \equiv -14144 \equiv 208896 \equiv 1048576 \equiv 1 \mod 41$:)

Next, for $\lambda = 7$ we have $p = 3, 13, 29$ their exponents f are $6, 2, 1$ respectively. An exponent of 6 means that the prime factors of 3 are just 3 time some units. That means that there is only one period of length 6 and as it is $\eta_0 = \alpha^6 + \alpha^5 + \cdots + \alpha = -1$ so it means that there can be no cyclic permutation. And if we insist of building $P(X)$ it will be of order X^6 and it actually won't work because substituting $X = \alpha$ will just give you zero because $\eta_0 = -1$.

But this actually hints that we cannot factor $X^6 + X^5 + \cdots + 1 \equiv 0 \mod 3$ and the hint says that the number of factors is e where in this case is 1. Indeed since the prime factor of 3 is just 3 times some unit if we can factor the above one of its factor has to be a multiple of 3 which means that the whole thing is a multiple of 3. Or at leaast we cannot factor it using this method.

For 13 its exponent $f = 2$ so $e = 6$, expect 6 factors. The $P(X)$ is $X^2 - \eta_0 X + 1$, from Table 4.7.5 the possible values are $-3, -5, -6$ rotating the three we get

$$(X^2 + 3X + 1)(X^2 + 5X + 1)(X^2 + 6X + 1) = X^6 + 14X^5 + 66X^4 + 118X^3 + 66X^2 + 14X + 1$$

where $14 \equiv 66 \equiv 118 \equiv 1 \mod 3$.

For 29 the exponent $f = 1$ so $e = 6$ but again this is like the case of $p = 41, \lambda = 5$, the $P(X) = 0$ so we need to do something similar to what we did with $p = 41$. From Page 100 we know that the prime factor of 29 divides $\alpha + 4$ so again in this case $\alpha \equiv -4$, other conjugates of prime factor of 29 are in $(\alpha^2)^4 \equiv (-4)^4$, $(\alpha^3)^5 \equiv (-4)^5$, $(\alpha^4)^2 \equiv (-4)^2$, $(\alpha^5)^3 \equiv (-4)^3$, $(\alpha^6)^6 \equiv (-4)^6$

$$\begin{aligned}(X - (-4))(X - (-4)^4)(X - (-4)^5)(X - (-4)^2)(X - (-4)^3)(X - (-4)^6) \\ = X^6 - 3276X^5 - 3581760X^4 + 899297280X^3 + 58683555840X^2 - 879394553856X \\ - 4398046511104\end{aligned}$$

and as usual the coefficients are all $\equiv 1 \mod 29$.

The last part of the question is factoring $X^{30} + X^{29} + \cdots + 1 \mod 2$. The exponent is $f = 5$ with $e = 6$. We don't have η for $\lambda = 31$. If we calculate $P(X)$ we get $X^5 - \eta_0 X^4 + (\eta_1 + \eta_2)X^3 - (\eta_4 + \eta_5)X^2 + \eta_3 X - 1$.

And since it is mod 2 the only choices for u will be $0, 1$. So there are only $2^6 = 64$ combinations to try for these η's.And a combination that works is $\eta_0 = 1, \eta_1 = 1, \eta_2 =$

$0, \eta_3 = 1, \eta_4 = 0, \eta_5 = 0$

$$(X^5 + X^3 - 2X^2 - 1)(X^5 + X^3 - X^2 + X - 1)(X^5 + 2X^3 - X^2 - 1) \times$$
$$(X^5 - X^4 - X^2 + X - 1)(X^5 - X^4 + X^3 + X - 1)(X^5 - X^4 + X^3 - X^2 - 1)$$

resulting in

$$X^{30} - 3X^{29} + 9X^{28} - 23X^{27} + 47X^{26} - 93X^{25} + 161X^{24} - 263X^{23} + 399X^{22} - 561X^{21} +$$
$$759X^{20} - 949X^{19} + 1141X^{18} - 1295X^{17} + 1389X^{16} - 1439X^{15} + 1389X^{14} - 1295X^{13} +$$
$$1141X^{12} - 949X^{11} + 759X^{10} - 561X^9 + 399X^8 - 263X^7 +$$
$$161X^6 - 93X^5 + 47X^4 - 23X^3 + 9X^2 - 3X + 1$$

and every coefficient is odd thus it is equivalent to $X^{30} + X^{29} + \cdots + 1 \mod 2$.

Note that in solving this problem we don't care about the factorization of p itself, as mentioned above in the exercises choosing different $\eta_i \equiv u_i$ generate different factorizations. What we need is just the integers u_i.

Page 125, Problem 4. We are counting the number of incongruent cyclotomic integers mod $h(\alpha)$ and it should be a power of p. This is similar to the counting of the number of incongruent nonzero elements of S on Page 124. The difference here is that we also include zero.

Following the hint, we start with p incongruent integers $0, 1, 2, \ldots, p-1 \mod h(\alpha)$. If these exhaust the number of incongruent integers mod $h(\alpha)$ then we are done. If not then there is $g_1(\alpha)$ incongruent to all these then $a + bg_1(\alpha)$ are incongruent to each other, these already include $0, 1, 2, \ldots, p-1$ because $0 \leq a, b < p$. How do we know that they are incongruent among themselves? if b is zero then it's obvious if a is zero then if $b'g_1(\alpha) \equiv b''g_1(\alpha)$ then $b' \equiv b''$ but if $b' \neq b''$ then it's not possible.

How many numbers do we have now? Since $0 \leq a, b < p$ we have p^2 incongruent numbers. If these exhaust everything we are done if not then we have another $g_2(\alpha)$ incongruent to all these and $a + bg_1(\alpha) + cg_2(\alpha)$, $0 \leq a, b, c < p$ are the new set of incongruent integers and there are p^3 of them. They are all incongruent because

$$a' + b'g_1(\alpha) + c'g_2(\alpha) \equiv a'' + b''g_1(\alpha) + c''g_2(\alpha) \mod h(\alpha)$$
$$\rightarrow (a' - a'') + (b' - b'')g_1(\alpha) \equiv (c'' - c')g_2(\alpha) \mod h(\alpha)$$

but this is inconsistent with the fact that

$$A + Bg_1(\alpha) \not\equiv g_2(\alpha) \mod h(\alpha)$$
$$\to (CA) + (CB)g_1(\alpha) \not\equiv Cg_2(\alpha) \mod h(\alpha)$$

for any $C \neq 0$ therefore they are all incongruent. And so on and so on :)

Page 125, Problem 5. We want to see which primes in Table 4.7.2 divide $7\alpha^3 + 45\alpha^2 + 83\alpha + 90$ (note that we are not factoring this thing just finding out which prime factor divides it). Note that Table 4.7.2 is $\lambda = 5, f = 2$. Since this problem is in Section 4.8 we should use what we learn in this section to solve this, no brute forcing :)

First we need to massage the cyclotomic integer into $g_1(\eta)\alpha + g_2(\eta)$ like on Page 122. We then substitute $\eta_i \equiv u_i$ and see if the resulting $a_1\alpha + a_2 \equiv 0h(\alpha)$ where $a_i = g_i(u)$.

For this we need $P(X)$ and for $\lambda = 5, f = 2$ it is simple enough $P(X) = X^2 - \eta_0 X + 1$ and so $\alpha^2 = \eta_0\alpha - 1$ and $\eta_0^2 = \eta_1 + 2 = -1 - \eta_0 + 2 = 1 - \eta_0$ thus we have

$$7\alpha^3 + 45\alpha^2 + 83\alpha + 90 = \alpha(38\eta_0 + 83) + (45 - 7\eta_0)$$

We now go to Table 4.7.2 at heeding the hint, we need to also check the conjugates, say for the first line of the table $\theta_0 \equiv 4, \theta_1 \equiv -5$ the conjugate will have $\theta_1 \equiv 4, \theta_0 \equiv -5$ and so on. And the Theorem in the section says that each coefficient must be zero for the whole thing to be $\equiv 0 \mod h(\alpha)$. Another thing to note is that this Theorem only applies to cyclotomic integers with degree less than f, this is why we need to massage it above. So we look for $38u_0 + 83 \equiv 45 - 7u_0 \equiv 0 \mod p$.

Trying out different rows from the table we get 29 and 79 as the factors with $\theta_0 \equiv -6$ for 29 and $\theta_0 \equiv 29$ for 79.

Page 125, Problem 6. I was initially confused by this. I think the *if only if* part only applies to the property of $Q_h(\alpha)$ not to the existence of it. Because otherwise the only if part will read *if* $g(X) = q(X)Q_h(X) + r(X)$ *with each coefficient of* $r(X) \equiv 0 \mod p$ *then there is* $Q_n(\alpha)\ldots$ which doesn't make sense since we already used $Q_h(X)$ before proving that it exists.

So basically what it's asking is that we can always find $Q_h(\alpha)$ with the property that if $h(\alpha)|g(\alpha)$ then $g(X) = q(X)Q_h(X)+r(X)$ where coefficients of $r(X)$ are all $0 \mod p$ and that if $g(X) = q(X)Q_h(X) + r(X)$ with coefficients of $r(X) \equiv 0 \mod p$ then $h(\alpha)|g(\alpha)$.

Well, this $Q_h(\alpha)$ is $P(\alpha)$ and we are done :) well almost, we need to replace each period with its counterpart u_i then we are really done.

Page 127. Comment on Theorem 1 especially on "the new definition coincides with the old one whenever the old one is valid". If you see the proof of Theorem 1 on Page 129 and Page 130 you'll see that the equivalence relation mod a prime factor $h(\alpha)$ is defined as $\cdot\Psi(\eta) \equiv \cdot \mod p$.

How do we derive congruence modulo a prime factor $h(\alpha)$ from this? Well

$$\begin{aligned} f(\alpha)\Psi(\eta) &\equiv 0 \mod p \\ \rightarrow f(\alpha)\Psi(\eta) &\equiv 0 \mod h(\alpha) \end{aligned}$$

since $h(\alpha)$ is prime it either divides $f(\alpha)$ or $\Psi(\eta)$. The key here is that $h(\alpha)$ must not divide $\Psi(\eta)$ and this is guaranteed because if $h(\alpha)|\Psi(\eta)$ it means that being prime it divides $\eta_i - j$ in $\Psi(\eta)$. But $\eta_i \equiv u_i \not\equiv j \mod h(\alpha)$.

If $h(\alpha)$ divides $\eta_i - j$ then we will have $u_i - j \equiv 0 \mod h(\alpha)$ which means that $h(\alpha)$ divides a number less than p that is co-prime to p since p is a prime integer but this is impossible since $Nh(\alpha)|p^{\lambda-1}$ while $h(\alpha)|j - u_i$ means $Nh(\alpha)|(j-u_i)^{\lambda-1}$.

How about the other way around? can two prime factors $h_1(\alpha)$ and $h_2(\alpha)$ divide the same $\eta_i - u_i$? Since p is a normal integer having cyclotomic prime factors means that

$$p = h_1(\alpha)h_2(\alpha)\cdots h_n(\alpha)$$

must be invariant under any conjugation. This means that we must have the $h_i(\alpha)$ to be conjugates of one another and we must have all conjugates of $h_i(\alpha)$ so that the RHS is invariant under any conjugation. One option is to have $n = \lambda - 1$ prime factors each a conjugate of the other.

But if this is the case then the RHS is just $Nh_1(\alpha)$ but if this is the case then we have what is described in Page 92 which is a prime that divides a binomial.

For n less than $\lambda - 1$ distinct prime factors we still have them to be a cyclic permutation themselves under any conjugation, however, if we take the norm of $h_1(\alpha)$ we will then get

$$\begin{aligned} Nh_1(\alpha) &= h_1(\alpha)h_2(\alpha)\cdots h_{n<\lambda-1}(\alpha) \times \{\lambda - 1 - n \text{ conjugates}\} \\ &= p \times \{\lambda - 1 - n \text{ conjugates}\} \end{aligned}$$

but the LHS is just a normal integer so the curly braces must be a normal integer too. But since we don't have all the conjugates of $h_1(\alpha)$ in this curly braces it is not invariant under any conjugation and therefore cannot be an integer.

What this means is that $n|\lambda - 1$ and

$$p = \{h_1(\alpha)h_2(\alpha)\cdots h_n(\alpha)\}^m$$

But in this case the norm of $h_1(\alpha)$ is $Nh_1(\alpha) = \{h_1(\alpha)h_2(\alpha)\cdots h_{e-1}(\alpha)\}^l$ where $l = \frac{\lambda-1}{n}$. But if $l < m$ then obviously $Nh_1(\alpha)|\{h_1(\alpha)h_2(\alpha)\cdots h_n(\alpha)\}^m$ which means $Nh_1(\alpha)|p$ but since p is a prime integer this means that $Nh_1(\alpha) = p$ and $l = m$ (we have assumed that $h(\alpha)$ is not a unit). This case is of no interest because $Nh_1(\alpha) = p$ is again covered by the Theorems on Page 92.

If $m < l \rightarrow l = mq + r$ then

$$Nh_1(\alpha) = p^q \cdot \{h_1(\alpha)h_2(\alpha)\cdots h_n(\alpha)\}^r$$

The curly braces is invariant under any conjugation and therefore it must be an integer but from the definition $p = \{h_1(\alpha)h_2(\alpha)\cdots h_n(\alpha)\}^m$ above $\{h_1(\alpha)h_2(\alpha)\cdots h_n(\alpha)\}^r|p$ and since p is a prime integer this cannot be unless $r = 0$ and in this case we have $Nh_1(\alpha) = p^q$.

We are almost done, this means that the prime factors of a prime integer must be a conjugate of one another and since $\eta_i \equiv u_i \mod h_1(\alpha)$ means that $\sigma^k\eta_i = \eta_{i+k} \equiv u_i \mod h_1(\sigma^k\alpha)$ and so the same $\eta_i \equiv u_i$ cannot be shared by two different prime factors.

Another note about Theorem 1 is that we have actually many $\Psi(\eta)$ one for each prime factor $h_i(\alpha)$ of p. If for one prime factor $\Psi(\eta) \not\equiv 0 \mod h_i(\alpha)$ then it must be 0 for the other prime factors as discussed above since no two prime factors can share the same $\eta_i \equiv u_i$ and no two $\eta_j \equiv u_j$ is established by the same prime factor.

In conclusion, every prime factor $h_i(\alpha)$ has its own $\Psi_i(\eta)$ which it doesn't divide and so the congruence $f(\alpha)\Psi_i(\eta) \equiv 0 \mod p$ means that $f(\alpha) \equiv 0 \mod h_i(\alpha)$ and so the two congruences coincide if there is an actual prime factor.

Page 128. Bottom page, proof of Proposition. Possible values mod p now has more than just $0, 1, 2, \ldots, p-1$ this is because cyclotomic integers are also included otherwise it's very easy to prove that we can find a unique u_i mod p for each η_i. This is because if there are only p valid values mod p like above then $j - \eta_i$ can only take p different values

mod p and all of them must be unique because otherwise $j_1 - \eta_i \equiv j_2 - \eta_i$ means $j_1 \equiv j_2$ mod p. And the proof of the Proposition is immediately completed :)

Page 128. My summary on the proof of the Proposition. I was initially very confused by all this. The key is to remember that prime integers are no longer cyclotomic prime in general. Another thing to note is that no $j - \eta_i$ is actually divisible by p.

This latter fact is because for a cyclotomic integer to be divisible by an integer a all of its coefficients must have the same value mod a as noted on Page 85. But a period's coefficients are just 0 and 1 (except for periods with length $\lambda - 1$). And so $j - \eta_i$ has coefficients of $j, 0, -1$ which can't be made to be equal to each other mod p.

The other thing I couldn't initially understand was how and why we need $\Psi(\eta)$. If we are right that none of $j - \eta_i$ is divisible by p then how do we get $j - \eta_i \equiv 0 \mod p$? The answer is we don't. What we have is $(j - \eta_i)\Psi(\eta) \equiv 0 \mod p$.

The whole product is zero not individual terms, again this is because p is not longer prime and so the product can be divisible by p while each term is not. And this is why we need $\Psi(\eta)$ because we can't have individual terms to be 0 mod p.

Having cleared this confusion let's see an example on how to build $\Psi(\eta)$. First problem I had was how do I chose which $j-\eta$ to start with, how do I know which one is not divisible by p. But according to my understanding above each $j - \eta$ is not divisible by p so we can choose anyone. But if that's the case what will happen if we actually start with the actual $u - \eta$ as a starting point and will it still work. If $u - \eta$ is part of $\Psi(\eta)$ why is $\Psi(\eta)$ not divisible by p?

Another thing I was confused about was that a cyclic permutation of the u's is also a solution. Doesn't it mean that there are two u's for each η? But the proof explicitly says that there is only one u for each η. Let's see this with an example.

Take $\lambda = 5$ and $p = 19$, in Section 4.7 we know that the prime factors of 19 is $(\eta_0 - 4)(\eta_1 - 4)$ or $(\eta_0 + 5)(\eta_1 + 5)$, in the first case we have $\eta_0 \equiv 4, \eta_1 \equiv -5$ and in the second case we have $\eta_0 \equiv -5, \eta_1 \equiv 4$.

We can start with **any** $j - \eta$ we want. Say we start with $\Psi(\eta) = \eta_0 - 4$. Even though $\eta_0 \equiv 4$ is one of the solution for u this is fine. What this means is that with this choice of $\Psi(\eta)$ we can't have $\eta_0 \equiv 4$ because $(\eta_0 - 4)\Psi(\eta)$ can not be 0 mod p. Another thing this

decides is $\eta_1 \equiv 4$ (which means $\eta_0 \equiv -5$) because $(\eta_1 - 4)\Psi(\eta) = (\eta_0 - 4)(\eta_1 - 4) = 19 = p$. Which means that $\eta_1 \not\equiv -5$. A starting point of $\Psi(\eta) = \eta_1 + 5$ will also produce the same η_0.

Had we started with $\Psi(\eta) = \eta_1 - 4$ then we automatically set $\eta_0 \equiv 4$ and $\eta_1 \equiv -5$. But in this case we have a different $\Psi(\eta)$ from our previous choice. Of course, with this choice, for the next step we cannot include $\eta_0 - 4$ in $\Psi(\eta)$.

What this means is that if $\Psi(\eta)$ already contains one set of the u's then it will not accept another one. In other words, for every set of u, in the first example above $\eta_0 \equiv -5, \eta_1 \equiv 4$, we have a unique $\Psi(\eta)$. So for each cyclic permutation we have a new $\Psi(\eta)$.

Another note on this Proposition is that it does not establish the congruence relations $\eta_1 \equiv u_i$. This is because the congruence relation mod a prime factor is not defined yet. The congruence relation is defined only in Theorem 1. What this proposition says is that if we have an equation $F(\eta_0, \eta_1, \eta_2, \dots) = 0$ then we will have $F(u_0, u_1, u_2, \dots) \equiv 0 \mod p$.

Why is this important? because it means that we still cannot do substitution for the η's. For example, we have $\phi(\eta) = \eta_0 + 3\eta_1$ we can't just say $\phi(u) = u_0 + 3u_1$ because again the congruence relation $\eta_i \equiv u_i$ is not established yet. However, if we have $\eta_0 + 3\eta_1 = 0$ then we can say that $u_0 + 3u_1 \equiv 0 \mod p$.

Another note, from the proof of the Theorem on Page 112 we see that as long as $g(\alpha)$ is made up of periods of length f we have the prime factor $h(\alpha)|[g(\alpha) - j]$. Therefore instead of using $j - \eta_i$ we can use $j - \phi(\eta)$ where $\phi(\eta)$ is made up of periods of length f. But we need e of them, one thing we can do is $\phi_i(\eta) = \sigma^i \phi(\eta)$.

We will then get

$$(\phi_i(\eta) - j)\Gamma(\phi) \equiv 0 \mod p$$

where $\Gamma(\phi)$ plays the role of $\Psi(\eta)$. But what it means is that we won't get $\eta_i \equiv u_i$ but rather $\phi_i(\eta) \equiv v_i$.

Now how does this relate to $F(\eta) = 0 \to F(u) \equiv 0 \mod p$? Any $F(\phi) = 0$ can be converted into $F(\eta) = 0$, inserting u (or one of the cyclic permutation of u) for η we must have $F(u) \equiv 0$. Now assume that $\phi_i(\eta) \to v_i$ implies another assignment $\eta_i \to w_i$ where w is not part of the cyclic permutation of u. Then when we convert $F(\phi) = F(\eta)$ and

substitute $F(\eta \to w)$ since $F(\phi \to v) = F(\eta \to w)$ and $F(\phi \to v) \equiv 0$ we must have $F(\eta \to w) \equiv 0$ as well but this is in contradiction to Theorem 2 that states that any $\overline{u}$ must be a cyclic permutation of u. Thus any $\eta \to w$ implied by $\Psi \to v$ must be a cyclic permutation of the u.

Page 133. Top page, the manipulation of $\sigma^{-k}\Psi(\eta)$ is very similar to the one usually done to the Euler totient function $\phi(p^n)$ that counts the number of co-prime numbers less than p^n, we can multiply everything and then divide by the ones that shouldn't be there, see Apostol for detail.

Page 133. Top page, last part of proof of Theorem 2. Note that we went through all these hoops because what we have is $g(\alpha)\Psi(\eta) \equiv 0 \mod p$ and what we want is $g(\alpha) \equiv 0 \mod p$. Again, p though a prime is not cyclotomic prime so we can't say that $p|g(\alpha)$ or $p|\Psi(\eta)$ from $g(\alpha) \equiv 0 \mod p$.

If what we have is $g(k)\Psi(u) \equiv 0 \mod p$ then we can handle it like normal integers because now they are normal integers but what we have here is $g(\alpha)\Psi(\eta)$ which is a cyclotomic integer.

Another thing to note is as my note above on the Proposition on Page 126, for each set of u's (for each different prime factor of p) we have a different $\Psi(\eta)$. And this proof shows that the different $\Psi(\eta)$'s are related to one another by $\sigma^{-k}\Psi(\eta)$.

Page 133, Problem 1. We want to build $\Psi(\eta)$ for $\lambda = 31$ and $p = 2$ ($f = 5$, $e = 6$). Since we are working mod 2 the values of u can only be 0 or 1. From Section 4.7, Page 120, the multiplication table indicates that $u_0, u_1, \ldots, u_5$ must have two consecutive 1's or two consecutive 0's, *i.e.* $1, 1, 0, 0, 1, 0$ or $0, 0, 1, 0, 1, 1$.

Let's start with the consecutive 1's as a guess for our $\Psi(\eta)$. This choice gives us

$$\Psi(\eta) = (\eta_0 - 0)(\eta_1 - 0)(\eta_2 - 1)(\eta_3 - 1)(\eta_4 - 0)(\eta_5 - 1)$$

what we need to check if this is not 0 mod 2 and if multiplying it with our choice of u's will make it 0 mod 2. The result is

$$\Psi(\eta) = 1 + \eta_1 + \eta_3 + \eta_4$$

which is clearly not 0 mod 2. Now let's check the result of $(\eta_i - u_i)\Psi(\eta)$

$$\begin{aligned}
(\eta_0 - 1)\Psi(\eta) &= 4 + 4\eta_0 + 2(\eta_2 + \eta_3 + \eta_4 + \eta_5) &&\equiv 0 \mod 2\\
(\eta_1 - 1)\Psi(\eta) &= 4 + 4\eta_2 + 2(\eta_0 + \eta_1 + \eta_3 + \eta_5) &&\equiv 0 \mod 2\\
(\eta_2 - 0)\Psi(\eta) &= 4(\eta_0 + \eta_1) + 2(\eta_2 + \eta_3 + \eta_4 + \eta_5) &&\equiv 0 \mod 2\\
(\eta_3 - 0)\Psi(\eta) &= 4(\eta_3 + \eta_5) + 2(\eta_0 + \eta_1 + \eta_2 + \eta_4) &&\equiv 0 \mod 2\\
(\eta_4 - 1)\Psi(\eta) &= 4 + 4\eta_5 + 2(\eta_0 + \eta_1 + \eta_2 + \eta_4) &&\equiv 0 \mod 2\\
(\eta_5 - 0)\Psi(\eta) &= 4(\eta_2 + \eta_4) + 2(\eta_0 + \eta_1 + \eta_3 + \eta_5) &&\equiv 0 \mod 2
\end{aligned}$$

Page 120 also says that the guess with two consecutive 1's or 0's doesn't mean that these u's satisfies all relations among the η's but the Proposition of Section 4.9 will prove this. And this problem proves that $1, 1, 0, 0, 1, 0$ works for all relations among η's, *i.e.* what it takes is to find $\Psi(\eta)$ that works.

Page 133, Problem 2. This time we find $\Psi(\eta)$ for $\lambda = 13$ and $p = 3$ ($f = 3$, $e = 4$). We are working with mod 3 so the possible values for u are $-1, 0, 1$. From Section 4.7 Page 120, one possible values for the u's are $0, -1, -1, 1$ with this choice of u we have

$$\begin{aligned}
\Psi(\eta) &= \{(\eta_0 + 1)(\eta_0 - 1)\}\{(\eta_1 - 0)(\eta_1 - 1)\}\{(\eta_2 - 0)(\eta_2 - 1)\}\{(\eta_3 + 1)(\eta_3 - 0)\}\\
&= 2\eta_0 + \eta_1 + 2\eta_3
\end{aligned}$$

which is clearly not 0 mod 3. Now we check the products with $\eta_1 - u_i$

$$\begin{aligned}
(\eta_0 - 0)\Psi(\eta) &= 6\eta_2 + 3(\eta_0 + \eta_1 + \eta_3) &&\equiv 0 \mod 3\\
(\eta_1 + 1)\Psi(\eta) &= 6 + 6(\eta_0 + \eta_3) + 3(\eta_1 + \eta_2) &&\equiv 0 \mod 3\\
(\eta_2 + 1)\Psi(\eta) &= 6 + 6(\eta_1 + \eta_3) + 3(\eta_0 + \eta_2) &&\equiv 0 \mod 3\\
(\eta_3 - 1)\Psi(\eta) &= 3 + 3(\eta_0 + \eta_1 + \eta_2) &&\equiv 0 \mod 3
\end{aligned}$$

Page 133, Problem 3. We want to prove that when the exponent of p mod λ is $\lambda - 1$ then p is prime cyclotomic integer. The hint says that what we need to do is prove that the Proofs in this Section 4.9 apply when $e = 1$.

From Page 114 and 116 of Section 7 we know that the factors of p are p times units, there it was mentioned that the prime factor of p is units times p but the argument actually applies to just a factor of p not necessarily prime factors of p.

Showing that the proofs in this section apply to $e = 1$ means that the ideal prime factor of p has all the properties defined through the Proposition and Theorems of Section 4.9. However, this does not prove that the prime factor of p actually exists.

But adherence to the Proposition and Theorems in this Section means that we can define an equivalence relation mod a prime factor of p that applies to cyclotomic integers $f(\alpha) \equiv g(\alpha) \mod h(\alpha) \Leftrightarrow f(\alpha)\Psi(\eta) \equiv g(\alpha)\Psi(\eta) \mod p$ but more importantly that this equivalence relation is prime. Furthermore, Theorem 2 states that there is only one distinct equivalence relation of this type.

But the catch is that this equivalence relation is mod the prime factor of p and not mod p. However, the second half of Theorem 2 states that $g(\alpha) \equiv 0 \mod p \Leftrightarrow g(\alpha)\Psi(\eta) \equiv 0 \mod p \Leftrightarrow g(\alpha) \equiv 0 \mod h(\alpha)$ as long as $g(\alpha) \equiv 0$ mod all prime factors of p.

We still have not proved that there is a prime factor of p and we have not proved that that prime factor is p itself but we already have what we need thanks to the last part of Theorem 2.

Say $f(\alpha)g(\alpha) \equiv 0 \mod p$ then thanks to Theorem 2, *i.e.* $w(\alpha) \equiv 0 \mod p \Leftrightarrow w(\alpha) \equiv 0 \mod h(\alpha)$, we have $f(\alpha)g(\alpha) \equiv 0 \mod h(\alpha)$ and Theorem 1 says that this latter congruence is prime, $f(\alpha) \equiv 0 \mod h(\alpha)$ or $g(\alpha) \equiv 0 \mod h(\alpha)$. Using the $\Leftrightarrow$ from Theorem 2 again we immediately get $f(\alpha) \equiv 0 \mod p$ or $g(\alpha) \equiv 0 \mod p$ which means that p is a cyclotomic prime.

One might ask, if that's the case then p is always cyclotomic prime even if $e > 1$. Not so fast. Say there are 2 ideal prime factors $h_1(\alpha), h_2(\alpha)$ corresponding to $e = 2$. Then Theorem 2 brings our mod p to $h_1(\alpha)|f(\alpha)$ or $h_1(\alpha)|g(\alpha)$ and $h_2(\alpha)|f(\alpha)$ or $h_2(\alpha)|g(\alpha)$. The problem is if $h_1(\alpha)|f(\alpha)$ but $h_2(\alpha) \nmid f(\alpha)$ (so $h_2(\alpha)|g(\alpha)$) then we can't bring it back to $p|f(\alpha)$ because the Theorem states that only if $f(\alpha)$ is divisible by both $h_1(\alpha)$ and $h_2(\alpha)$ then we can say that $f(\alpha) \equiv 0 \mod p$. But for $e = 1$ there's only one ideal prime factor so this complication never arises.

Note that in the above reasoning the existence of an actual prime factor of p is not needed. Also that to prove Theorem 2 we need the Proposition and Theorem 1. Therefore to solve this Problem we need to show that the proofs of the Proposition and Theorems apply for $e = 1$.

First the Proposition on Page 126. Now there is only one u and one η, *i.e.* η_0 and u_0. We need to show that we can find u_0 such that $\eta_0 - u_0 \equiv 0 \mod p$. For this we don't actually need $\Psi(\eta)$ because

$$\eta_0 = \alpha^{\lambda-1} + \alpha^{\lambda-2} + \cdots + \alpha$$

and as mentioned many times above for a cyclotomic integer to be divisible by an integer all of its coefficients must be the same modulo that integer. Here that integer is p and as long as $-u_0 \equiv 1 \mod p \rightarrow u_0 = p - 1$ we will have $\eta_0 - u_0 = \eta_0 + 1 \equiv 0 \mod p$.

One might be tempted to say that we don't need $\Psi(\eta)$ because p is now no longer just an integer prime but also a cyclotomic prime since the only factors of p are p itself. But this is already assuming that p is already a cyclotomic prime something that we want to achieve so we can't do this.

Nevertheless, $\Psi(\eta)$ is easily found (and there's only one of it)

$$\Psi(\eta) = \prod_{j=1}^{p-2}(\eta_0 - j) \not\equiv 0 \mod p$$

The fact that it is $\not\equiv 0 \mod p$ is not due to the fact that each term is not divisible by p (due to the fact that the coefficients are not the same mod p) therefore the whole product is not divisible by p either. We can't say this because this assumes that p is prime cyclotomic. The reason it is $\not\equiv 0$ is what was shown in the book.

Proof of Theorem 1 doesn't depend on e at all and so it still applies in this case and the equivalence relations $f(\alpha) \equiv g(\alpha)$ are still defined as $f(\alpha)\Psi(\eta) \equiv g(\alpha)\Psi(\eta)$.

Proof of Theorem 2. The crux of Theorem 2 is the last paragraph on Page 131. But in this case there's only one e therefore we don't need to go through all this hoops, if there's another $\overline{u}_0$ then it must be $\equiv u_0$ because there's only one of them (note that mod 1 everything is zero so the statement on Page 132 $k \equiv 0 \mod e = 1$ is meaningless here)and here $M = \Psi(\eta)$. Again, the proof of the last part of Theorem 2 is also trivial in this case because there's only $e = 1$ ideal prime factor of p. We immediately get $g(\alpha) \cdot M \equiv 0 \mod p$ of Page 133 nothing else needs to be done.

Page 133, Problem 4. We want to show that if a cyclotomic integer $\phi(\eta)$ is made up of periods f with norm p^f where f is the exponent of p mod λ then $\phi(\eta)$ is prime cyclotomic.

What we know is that since $N\phi(\eta) = p^f$ and

$$N\phi(\eta) = p^f = \{\phi(\eta) \cdot \sigma\phi(\eta) \cdot \cdots \cdot \sigma^{e-1}\phi(\eta)\}^f$$
$$\rightarrow \pm p = \phi(\eta) \cdot \sigma\phi(\eta) \cdot \cdots \cdot \sigma^{e-1}\phi(\eta)$$

the plus minus depends on whether e, f are even or odd. The reason we can group the norm like above is because $\phi(\eta)$ is made up of periods only and even though σ covers all conjugation of α, σ^e is the identity transformation for periods thus every e conjugations the pattern repeats. And the reason we define p that way is because p as an integer is invariant under any conjugation thus we must have all conjugates of $\phi(\eta)$ other choices of e conjugates of $\phi(\eta)$ are not be invariant under conjugation. For simplcity let's denote $\sigma^k\phi(\eta) \rightarrow \phi_k(\eta)$.

From Section 4.9 we know that p has prime divisors (although they mght be hypothetical) and Theorem 2 states that there are e of them, let's denote them and their corresponding hypothetical counterparts $h_i(\alpha) \leftrightarrow \Psi_i(\eta)$. One thing to note is that these e prime factors of p are conjugates of one another. We can see this from the fact that the $\Psi_i(\eta)$ are conjugates of one another as it is just a product of $j - \eta_l$ so a conjugation is just a cyclic permutation of the η's.

The prime divisors of p being prime must divide one (or more) of the conjugates $\phi_k(\eta)$ in the RHS. Say $\phi_k(\eta)\Psi_i(\eta) \equiv 0 \mod p$ a conjugation of this gives us

$$\sigma^j\phi_k(\eta)\Psi_i(\eta) = \phi_{k+j}(\eta)\Psi_{i+j}(\eta) \equiv 0 \mod p$$

So the situation now is each $\phi_i(\eta)$ is divisible by the same number of prime divisors of p. But if each $\phi_i(\eta)$ is divisible by n of the prime divisors then the product $\pm p = \prod \phi_i(\eta)$ is divisible by the e prime divisors n times which is not possible since p contains exactly the e prime divisors exactly once. Thus each $\phi_i(\eta)$ is divisible by exactly one prime divisor of p.

Another thing we need to consider is that $\phi_i(\eta)$ can be divisible by other factors whether prime or not. But if that's the case then these factor would divide p and therefore must divide p on top of its e prime factors which is not allowed (unless those factors are units). Thus each $\phi_i(\eta)$ only has one prime factor plus units.

We could've said that the norm of $h_i(\alpha)$ is the same as the norm of $\phi_k(\eta)$ and therefore each $\phi_k(\eta)$ only contains the corresponding prime factor and at most units but $h_i(\alpha)$ might not even exist.

Now since each $\phi_k(\eta)$ contains only one prime factor and at most units it must be prime as well (units times prime is also prime). The only question now is what happens if $h_i(\alpha)$ is actually non existent? That's fine because then it would mean that $\phi_k(\eta)$ is also hypothetical and congruence relations mod $\phi_k(\eta)$ is defined through $\Psi_i(\eta)$ as well.

But in this case since $\phi_k(\eta)$ satisfies the congruence relations $\cdot\Psi_i(\eta) \equiv \cdot \mod p$ and it also divides p therefore it must the a prime divisor of p.

Page 133, Problem 5. We need to show that the coefficients of $(X-\eta_1)(X-\eta_2)\dots(X-\eta_e)$ are all integers. The coefficients of X^e is 1 so it is an integer, the coefficient of X^0 is a product of $(-1)^e\eta_0\eta_1\eta_2\dots\eta_e$ and this is clearly invariant under σ^j because what σ^j does is j cyclic permutations, since the product contains all η's any cyclic permutation leaves it invariant.

For other coefficients, say that of X^i, it is made of all product of $e-i$ number of η's, *i.e.* e choose i η's. Since it contains all possible combinations of e choose i eta, any cyclic permutations will leave it invariant. The only possible problem is that each term in the coefficient has a different sign from the other. But this is not so because each e choose i term will have $(-1)^i$ as its sign.

We now need to calculate all coefficients up to $\lambda = 13$, the only valid values for λ are $\lambda = 3, 5, 7, 11, 13$. Again, it's easier to write the Python script for this Problem :) But for the Python script it's easier to calculate it directly rather than trying to use the multiplication table.

```
def Page133Problem5(L):

    import itertools
    # we need to get all possible values of e

    for e in xrange(2,L):
        print 'e = %d' % e
        if (L-1) % e == 0:
            f = (L-1)/e

            eta = generateEtas(L,f)
            nz = findEtaNz(eta)

            # don't forget to set the minus sign
```

```
for i in xrange(e):
    eta[i] = [-1*j for j in eta[i]]

t = [i for i in range(0,e)]

for y in xrange(1,e+1):

    l = itertools.combinations(t, y)

    tot = [0] * L
    for i in l:
        # create individual products
        res = [0] * L
        res[0] = 1
        for j in i:
            res = multCyc(res, eta[j])

        tot = addCyc(tot, res)

    # check that tot has same elements from [1:end]
    for i in xrange(2,L):
        if tot[i] != tot[i-1]:
            print 'Something Wrong'
    else:
        print '%d*X^%d' % (tot[0] - tot[1], e - y)
```

The answers are

$\lambda = 3 \ , e = 2 \ \rightarrow X^2 + X + 1$

$\lambda = 5 \ , e = 2 \ \rightarrow X^2 + X + 1$

$\lambda = 5 \ , e = 4 \ \rightarrow X^4 + X^3 + X^2 + X + 1$

$\lambda = 7 \ , e = 2 \ \rightarrow X^2 + 2X + 3$

$\lambda = 7 \ , e = 3 \ \rightarrow X^3 + X^2 - 2X - 1$

$\lambda = 7 \ , e = 6 \ \rightarrow X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$

$\lambda = 11 \ , e = 2 \ \rightarrow X^2 + X + 3$

$\lambda = 11 \ , e = 5 \ \rightarrow X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$

$\lambda = 11 \ , e = 10 \ \rightarrow X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$

$\lambda = 13 \ , e = 2 \ \rightarrow X^2 + X - 3$

$\lambda = 13 \ , e = 3 \ \rightarrow X^3 + X^2 - 4X + 1$

$\lambda = 13 \ , e = 4 \ \rightarrow X^4 + X^3 + 2X^2 - 4X + 3$

$\lambda = 13 \ , e = 6 \ \rightarrow X^6 + X^5 - 5X^4 - 4X^3 + 6X^2 + 3X - 1$

$\lambda = 13 \ , e = 12 \ \rightarrow X^{12} + X^{11} + X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$

Something interesting here is that for $e = \lambda - 1$ we have $\sum_{i=0}^{\lambda-1} X^i$. This is obvious because the polynomial is $\prod_{i=1}^{\lambda-1}(X - \alpha^i)$ and any α^j is now a root but the constant factor is always

1 because it's the product of $(-1)^{\lambda-1}\prod_{i=1}^{\lambda-1}\alpha^i = (+1)\alpha^{\frac{\lambda(\lambda-1)}{2}} = 1$ so when we set $X = \alpha$ the sum of the powers of α must be -1 and the result follows.

Proposition 133.0 *The sum of all combinations of $m = \lambda - 1$ choose n of products of n α^j is $(-1)^n$.*

Proof. What is says is that, *e.g.* $m = 5 - 1 = 4$ and $n = 3$ then what we have is

$$\alpha^1\alpha^2\alpha^3 + \alpha^1\alpha^2\alpha^4 + \alpha^1\alpha^3\alpha^4 + \alpha^2\alpha^3\alpha^4 = -1$$

From the above solution to Problem 5 the answer is obvious. We can also prove this by counting and induction but it's very cumbersome. The idea is like so, let $m = 4$ like above and start with $n = 1$ in this case the sum is just $\sum_{i=1}^{4}\alpha^i = -1$ which is obvious. We then move to $n = 2$. To do this start with

$$(-1)^2 = (\alpha^4 + \alpha^3 + \alpha^2 + \alpha)^2 = (\alpha^3 + \alpha + \alpha^4 + \alpha^2) + 2(\text{cross terms})$$

The first bracket in the RHS is what I call the main term and it amounts to -1. The LHS is $+1$. The cross terms are what we want and so

$$2 = 2(\text{cross terms})$$

Thus the cross terms sum to 1 which is consistent with the Proposition. Next is $n = 3$, it's easier if we denote $x = \alpha, y = \alpha^2, z = \alpha^3, w = \alpha^4$. Again we start with

$$(-1)^3 = (x^4 + y^3 + z^2 + w)^3 = (x^2 + y^4 + x + w^3) + 3x^2(y + z + w) + \text{cyclic permutation} + 6(\text{cross terms})$$

The cyclic permutations on the RHS means $3y^2(x + z + w)$ and so on. What we see here is that the bracket in the $3\cdot^2(\cdot + \cdot + \cdot)$ term is just the cross term in m choose 1 minus the leading term outside the bracket. So for $3x^2(y + z + w)$ it is equal to $3x^2(-1 - x) = -3x^2 - 3x^3$, combining with other cyclic permutations we get

$$-3(x^2 + y^2 + z^2 + w^2) - 3(x^3 + y^3 + z^3 + w^3) = 3 + 3$$
$$= 6$$

The LHS is -1, the main term is also -1, the cyclic permutations add to $+6$ so

$$0 = 6 + 6(\text{cross terms})$$

Thus the cross terms add to -1. The same idea applies when we go to $n = 4$ the only difference this time is that the cyclic permutation terms are more complicated, we'll get something like

$$12x^2(yz + yw + wz) + \text{cyclic permutation}$$

This time the terms in bracket is just the cross terms for $n = 2$ without the leading term thus

$$12x^2(yz + yw + wz) = 12x^2(1 - xy - xz - xw) = 12x^2 - 12x^3(y + z + w)$$

and the last bracket on the RHS is the cross terms for $n = 1$ and so we can repeat the process. As we go to higher powers we will get things like this with something like $C \cdot x^2y^3(\text{crossterms})$ where the cross terms are from lower n and exclude x and y. As you can see this line of thinking gets very messy indeed and so I decided not to pursue a full proof with this not to mention having to calculate the exact numerical factors and make sure they add up to the factor of the actual cross term.

Page 133, Problem 6. Here we are trying to learn about Kummer's gap. Problem 5 gives us the polynomial $\phi(X)$ and Kummer's gap was in his attempt in showing that $\phi(u) \equiv 0 \mod p$ has e distinct solutions mod p.

Following the instructions in the book, we need to show that

$$\begin{aligned}&\phi(X-1)\phi(X-2)\dots\phi(X-p)\\ &\equiv [(X-\eta_1)^p - (X-\eta_1)]\,[(X-\eta_2)^p - (X-\eta_2)]\dots[(X-\eta_e)^p - (X-\eta_e)]\end{aligned}$$

From Theorem on Page 112 we have $X^p - X \equiv [X-1][X-2]\dots[X-p] \mod p$, applying this Theorem to $\phi(X-1)\phi(X-2)\dots\phi(X-p)$ after expanding each $\phi(X-j)$ and collecting terms with the same η_i we get the above congruence relation.

We then expand each square bracket

$$(X-\eta)^p \equiv X^p - \eta^p \equiv X^p - \eta$$

the first equivalence is from the fact that every coefficient of $(X-\eta)^p$ is a multiple of p except the first and the last, the second equivalence follows from the fact that η is a period of length f which is the exponent of p mod λ thus $\eta^p \equiv \eta$ therefore

$$(X-\eta)^p - (X-\eta) \equiv X^p - X \equiv (X-1)(X-2)\dots(X-p)$$

the last equivalence again follows from Theorem on Page 112. Thus we get

$$\phi(X-1)\phi(X-2)\dots\phi(X-p) \equiv (X-1)^e(X-2)^e\dots(X-p)^e \mod p$$

I was actually at a total loss as to what this Problem was about. After looking at it long enough, I think what Kummer was trying to show was that since $\phi(X) = \prod_{i=1}^{e}(j-\eta_i)$ has e distinct roots mod p then we can immediately establish $\eta_i \equiv u_i$. But the only thing he had was that the product $\prod_{j=1}^{p}\phi(X-j)$ has p distinct roots with each having multiplicity e and he concluded from this that each $\phi(X)$ must have e distinct roots but Problem 7 shows that this is not true since $\phi(X)$ itself might not even be of degree e.

The second thing that confuses me about the comment on coincident roots was that I thought we needed to show that $\phi(X-1) \not\equiv (X-1)^e \mod p$ and so on because then $\phi(X)$ does not have distinct roots. But what he's asking is that the product $\prod_{j=1}^{p}\phi(X-j)$ has p distinct roots with each having multiplicity e.

And this is what he meant by "*meaning* of the statement that $\phi(X)$ has e distinct roots mod p", *i.e.* the product $\prod_{j=1}^{p}\phi(X-j)$ having p distinct roots with each having multiplicity e.

Because of all this confusion I checked the answer and I think he made a mistake there and by he I mean Edwards and not Kummer. He started by saying that if a polynomial $\Psi(X)$ has a root r with multiplicity k then we can write $\phi(X) = Q(X)(X-r)^k$ where $Q(X=r) \not\equiv 0 \mod p$.

Here we want to show that the product $\prod_{j=1}^{p}\phi(X-j)$ is

$$\prod_{j=1}^{p}\phi(X-j) \equiv \prod_{j=1}^{p}Q(X-j)(X-j)^t \mod p$$
$$\prod_{j=1}^{p}(X-j)^e \equiv \prod_{j=1}^{p}Q(X-j)(X-j)^t \mod p$$

where $Q(X-j) \not\equiv 0 \mod p$ for any X. He then made the mistake by canceling both sides to get $\prod_{j=1}^{p}Q(X-j) \equiv \prod_{j=1}^{p}(X-j)^{e-t} \mod p$, he said that if $a(X)b(X) \equiv c(X)b(X) \mod p$ then $a(X) \equiv c(X) \mod p$ if $b(X) \not\equiv 0 \mod p$.

But here $\prod_{j=1}^{p}(X-j)$ is $0 \mod p$ for any integer X because it is a product of p consecutive integers thus we cannot cancel it from both sides. What we can say though is

that for any value of X the LHS is actually $0 \mod p^e$ while the RHS is $0 \mod p^t$ because $Q(X) \not\equiv 0 \mod p$ for any X. Therefore the only way this works is if $e = t$.

Page 134, Problem 7. We are going to refute Kummer's claim. Kummer's proof concludes with

$$(y-\eta)^p - (y-\eta) \equiv y^p - y \equiv 0 \mod p$$

the last equivalence is from Fermat's Little Theorem $y^p \equiv y \mod p$, the difference from Problem 6 is instead of using Theorem on Page 112 to express $y^p - y \equiv [y-1][y-2]\dots[y-p] \mod p$ Kummer concluded that $y^p - y \equiv 0 \mod p$. And so

$$\begin{aligned}\phi(y-1)\phi(y-2)\dots\phi(y-p) &\equiv (y^p-y)^e \mod p \\ &\equiv 0 \mod p^e\end{aligned}$$

We now need to construct a counter example where $\phi(y-1)\phi(y-2)\dots\phi(y-p) \equiv 0 \mod p^e$ but $\phi(X)$ has degree less than e. Hint says that we can take $p = 2, e = 3$.

One silly counter example would be $\phi(X) = 2(X-1)$ then

$$\begin{aligned}\phi(X-1)\phi(X-2) &= 2^2(X-2)(X-3) \\ \to \phi(y-1)\phi(y-2) &\equiv 0 \mod p^3\end{aligned}$$

but I'm not sure if this is legit :) Let's try another one that is actually legit $\phi(X) = (X-1)(X-3)$

$$\phi(X-1)\phi(X-2) = (X-2)(X-4)(X-3)(X-5)$$

this is because whatever X you'll get a product of 2 consecutive even numbers (if X is even you'll get it from $(X-2)(X-4)$ and if X is odd you'll get it from $(X-3)(X-5)$) and a product of two consecutive even numbers is a multiple of 8 because $2m(2m+2) = 4m(m+1)$ but one of m or $m+1$ is even so the whole thing is a multiple of 8. The thing that tripped me was the whole thing can be zero and I forgot that zero is a multiple of anything including p^e LOL

Page 134, Problem 8. Here we want to know why we can always solve u_i given the multiplication table of the periods. Especially that once we find one u we can easily find the rest.

The calculation always starts with solving one u usually u_0. Once we have this the rest of the multiplication table gives $u_0 u_i = \text{const.} + \sum_{i=0}^{e} a_i u_i$ which means that we just have a system of linear equation by substituting u_0 with the number we found for u_0. The hint also says that it is a necessary condition to find all the u's but it is not clear that the $u's$ have all the requires properties.

I think one of the properties is the fact that the u's give rise to another set of solutions under cyclic permutations. Another more important property is that the u's satisfy all relations satisfied by the eta's, *i.e.* $F(\eta_0, \eta_1, \ldots, eta_e) = 0 \rightarrow F(u_0, u_1, \ldots, u_e) \equiv 0 \mod p$.

Page 134, Problem 9. We want to show that there is at least one $j - \eta_i$ that is not 0 mod p. Note that $1 \leq j \leq p$ and $1 \leq i \leq e$. If all of them are zero then there must be $j_1 - \eta_i \equiv 0 \equiv j_2 - \eta_i$ with $j_1 \neq j_2$ (note that here we are concentrating on the same i). But this means that $j_i \equiv j_2$ but since $1 \leq j_1, j_2 \leq p$ this must means $j_1 = j_2$, a contradiction. Therefore not all of them are 0 mod p which means that at least one of them is not 0 mod p.

We can also show that actually none of them is divisible by p unless p itself is a cyclotomic prime which happens only when the exponent of p is $\lambda - 1 \rightarrow e = 1$. This is because divisibility of a cyclotomic prime by an integer i means that every coefficient of that cyclotomic integer is the same mod i.

If $e > 1$ then every coefficient of α^j in each period is either 0 or 1 and for $j - \eta_i$ the coefficients will be $-1, 0, j$ and they can't be equal each other mod p. The only exception is that when $e = 1$ then there's only one period which contains all powers of α where each coefficient is 1 so this time $j - \eta_0$ can be divisible by p if $j \equiv -1 \mod p$.

Page 134, Problem 10. I need to understand what it's actually asking :) Having prime divisors for p means that we have $\eta_i \equiv u_i \mod h(\alpha)$ with this we can express any cyclotomic integer as $g_1(\eta)\alpha^{f-1} + g_2(\eta)\alpha^{f-2} + \cdots + g_f(\eta)$ and we can replace the $g(\eta)$ with $g(u)$ where each $g(u)$ is between $0 \leq g(u) < p$ and therefore we have p^f of these cyclotomic integers mod $h(\alpha)$, see Page 123.

These cyclotomic integers now form a group under multiplication and addition (or a field) mod $h(\alpha)$ although cyclotomic integers in general do not form a group since except

for units the rest don't have inverses. This is similar to the situation for integers, 4^{-1} is not an integer but $4^{-1} \bmod p$ exists.

I'm not so sure about the connection to polynomials of degree f. One think I can see is that the cyclotomic integers mod $h(\alpha)$ are now of the form $a_1\alpha^{f-1} + a_2\alpha^{f-2} + \cdots + a_f$ which is a polynomial of degree $f-1$. But we also have $P(X)$ of Page 122 which is of degree f and it is $0 \mod h(\alpha)$.

But we have e prime factors of p so if we multiply these e number of $P(X)$ (substituting $\eta \equiv u$ for each prime divisor $h(\alpha)$) we get

$$\begin{aligned} P_1(X)P_2(X)\dots P_e(X) &\equiv 0 \mod h_1(\alpha)h_2(\alpha)\dots h_e(\alpha) \\ &\equiv 0 \mod p \end{aligned}$$

The LHS is obviously of order $ef = \lambda - 1$ but it must be $0 \mod p$ and for cyclotomic integers this means that all of the coefficients have the same value mod p. This is as close as I can get to $X^{\lambda-1} + X^{\lambda-2} + \cdots + 1$.

The question asks us to construct the (irreducible) polynomial of degree f ab initio. Note that he's not asking a factorization of $X^{\lambda-1} + X^{\lambda-2} + \cdots + 1$, the only condition on this polynomial is that it's of degree f and it divides $X^{\lambda-1} + X^{\lambda-2} + \cdots + 1 \bmod p$. Note that we did this in Problem 2 and Problem 3 of Section 4.8 using cyclotomic integers.

I'm not quite sure by what he meant by this, because we can always start with a generic polynomial of degree f with $f-1$ unknown (the constant is either 1 or -1) and then do long division but even then at the end of the long division you'll get just one equivalence for the $f-1$ variables.

So I'm going to skip this one for now and come back later.

Page 134, Problem 11. Let j be the integer $0 \le j < e$ for which α^{-1} lies in η_j. Show that $j = 0$ if f is even and $j = \frac{1}{2}e$ if f is odd.

What this means is that η_j contains the inverse of η_0 since η_0 is the only one that has α, note that η_j is not the inverse of η_0 as $\eta_j\eta_0 \neq 1$ sine we have cross terms.

We know that $\eta_0 = \sum_{i=0}^{f-1} \sigma^{ei}\alpha$ and $\sigma^{ei}\alpha = \alpha^{\gamma^{ei}}$ where γ is a primitive root mod λ. We also know that $\eta_j = \sigma^j\eta_0$ which means that $\eta_j = \sum_{i=1}^{f} \sigma^{j+ei}\alpha$ where $0 \le j < e$.

If $\sigma^{j+ei}\alpha = \alpha^{-1}$ we must have $\gamma^{j+ei} \equiv -1 \mod \lambda$ and since γ is a primitive root mod λ it must be that $j + ei = \frac{\lambda-1}{2}$. Can it be an odd multiple of $\frac{\lambda-1}{2}$, no because j is at most

$e-1$ and i is at most $f-1$ so $j+ei$ is at most $ef-1=\lambda-2$

$$j+ei=\frac{\lambda-1}{2}=\frac{ef}{2}$$
$$\rightarrow j=\frac{e(f-2i)}{2}$$

since $j<e$ we have $\frac{(f-2i)}{2}$ less than 1 or $f-2i<2$. But $0\leq i<f$ if f is even then the only solution is $i=\frac{f}{2}$ with $j=0$ and if f is odd then $i=\frac{f-1}{2}$ and $j=\frac{e}{2}$.

Page 138, Problem 1. This is almost the same as Problem 4 of Page 133. However, this time $g(\alpha)$ bears no assumption that it is made up of periods of length f. Here too we can use the fact that p has e prime divisors as dictated by Theorem 2 of Section 4.9.

This means that p^f has a total of $ef=\lambda-1$ prime divisors each with multiplicity f. The norm $Ng(\alpha)$ has a total of $\lambda-1=ef$ conjugations. From the fundamental theorem since $Ng(\alpha)|p^f$ and $p^f|Ng(\alpha)$ the multiplicities of the prime divisors for both $Ng(\alpha)$ and p^f must be exactly the same.

Since the multiplicities on both sides are equal and p^f only contains prime divisors of p then $Ng(\alpha)$ only contains prime divisors of p as well. The only exception is units, both sides may contain units aside from the prime divisors.

The only question now is whether some conjugates of $g(\alpha)$ have more than one prime divisors, since the number of conjugates (a total of ef) is the same as the number of prime divisors, if one of the conjugates contains more than one prime divisors some of them will contain none and thus those will be a multiple of units and have norm 1 but the norm of a conjugate of $g(\alpha)$ is the same as the norm of $g(\alpha)$ so it cannot be units. Thus each conjugate of $g(\alpha)$ contains exactly one prime divisor of p and nothing else sans units and $g(\alpha)$ itself is therefore prime.

Again, if the prime divisors are actually hypothetical then $g(\alpha)$ will also be hypothetical and its congruence relations will be defined through $\cdot\Psi(\eta)\equiv\cdot \mod p$.

The next part of the question asks us to show that $g(\alpha)$ divides $h(\alpha)$ μ times if and only if $h(\alpha)$ is divisible with multiplicity μ by the prime divisor of p that divides $g(\alpha)$.

One direction is easy. If $g(\alpha)$ divides $h(\alpha)$ μ times then from the fundamental theorem we know that $h(\alpha)$ must have the same number of prime divisors as $g(\alpha)$.

The converse is also quite easy, if $h(\alpha)$ is divisible by the prime divisor of p μ times then

since $g(\alpha)$ is just units times this prime divisor, the fundamental theorem immediately gives us that $g^{\mu}(\alpha)$ divides $h(\alpha)$ because $g(\alpha)$ contains the same number of prime divisors as $h(\alpha)$, we don't even need to mess around with units.

As a side note, to handle units we can multiply $\Psi(\eta)$ with the inverse of that unit, *e.g.* $g(\alpha)u^{-1}(\alpha)\Psi(\eta) \equiv 0 \mod p$ means that $g(\alpha)$ is divisible by a prime divisor times a unit $u(\alpha)$.

Page 139, Problem 2. This time we need to prove that if $Ng(\alpha) = p_1^{\mu_1} p_2^{\mu_2} \dots p_k^{\mu_k}$ is the ordinary factorization of the integer $Ng(\alpha)$ then, for each i, $g(\alpha)$ is divisible by exactly μ_i/f_i prime divisors of p_i.

Again we will be utilizing the fundamental theorem. Let's concentrate on one p_i, we know that it has e_i prime factors and so $Ng(\alpha)$ must have the same number of prime factors. So for each prime factor there are μ_i copies of them on the RHS.

More importantly Theorem 2 of Section 4.9 says that each prime factor is related to another through conjugation. $Ng(\alpha)$ is a product of all conjugates of $g(\alpha)$ if $g(\alpha)$ contains n (not necessarily distinct) prime factors of p_i then there will be a factor $p_i^{nf_i}$ on the LHS because the $\lambda - 1$ conjugations contain f copies of the cyclic permutations of the η's. Therefore equating the two $p_i^{nf_i} = p^{\mu_i} \rightarrow n = \mu_i/f_i$.

Page 139. Bottom page, this is a cool way of looking at zero. Instead of zero being nothing, here zero has everything, *i.e.* zero has every number (including) zero as a factor.

Page 140. Top page, about $47 \cdot 139$ having two different ways of factoring it. If you read the end Section 4.4 you'll see that one way is $N(1 + \alpha + \alpha^{-2}) = 47 \cdot 139$. Another way is the comment he made about 47 as a product of 11 conjugates of $h(\alpha)$ where $h(\alpha) = h(\alpha^{-1})$. The same goes for 139.

This is actually an example of the failure of unique factorization. Since 47 does not have prime factors its factorization is not unique.

Page 140. Theorem and its proof, note that here he's using the lower case $\psi(\eta)$ as a reverse of the upper case $\Psi(\eta)$ we've been using, please be aware, this is not a good choice of variable :)

Page 140. Theorem in the middle of the page. This is the reverse of $\Psi(\eta)$. Here we want something that is only divisible by $h(\alpha)$, the usual definition of $\Psi(\eta)$ is something

that is divisible by other prime factors of p but not by $h(\alpha)$. Here we want something that is only divisible by $h(\alpha)$ and not by other prime factors of p. Of course $h(\alpha)$ can be nonexistent.

Page 140. Proof of Theorem. there's a simple typo there, the first term of $\phi(\eta)$ is $\delta\Psi(\eta)$, it should have been $\sigma\Psi(\eta)$.

Page 141, Problem 1. The setting is that one of the u's, u_j is unique and so $u_j - \eta_0$ is divisible by one of the prime divisors of p exactly once and not divisible by any other primes divisors. We need to show that this is not the only case because $u_j + kp - \eta_0$ is also actually divisible exactly once by the same prime divisor and not by any other.

I think the set up is like this. We don't know how many times $u_j - \eta_0$ is divisible by this prime divisor but we know that it is only divisible by this one prime divisor. But we know that kp is divisible once by the any prime divisor as long as $k \not\equiv 0 \mod p$. Therefore, adding kp guarantees that the sum $u_j + kp - \eta_0$ is divisible by this prime divisor only once.

The same goes with $\phi(\eta)$, if it is divisible by just one prime divisor (but maybe multiple times) then adding kp will restrict it to be divisible only once because kp is as long as $k \not\equiv 0 \mod p$.

As a side note, it might be odd to find out that some $\eta_i - u_i$ is divisible by a prime divisor more than once but for a concrete example the prime divisor associated with $\Psi(\eta)$ found in Problem 2 of Page 133 for $\lambda = 13$ and $p = 3$ actually divides $\eta_0 + 1$ twice.

Page 142, Problem 2. We actually calculated the capital letter $\Psi(\eta)$ for $\lambda = 31, p = 2 \to f = 5, e = 6$ in Problem 1 of Page 133. Here we need to find the lower case $\psi(\eta)$ defined on Page 140. There are only 6 prime divisors. First we find $\phi(\eta) = \sigma\Psi(\eta) + \sigma^2\Psi(\eta) + \cdots + \sigma^{e-1}\Psi$, $\Psi = 1 + \eta_1 + \eta_3 + \eta_4$ and we have $\phi(\eta) = 3 + \eta_0 + \eta_2 + \eta_5$.

We can just add p to $\phi(\eta)$ to make sure it is only divisible once by the prime divisor in question but let's check it out explicitly by multiplying it by $\Psi^\mu(\eta)$. And in this case I found that $\phi(\eta)$ is divisible by any multiplicities of $p = 2$ as I keep multiplying it by $\Psi^\mu(\eta)$ the result is always divisible by 2^μ. Thus we need to add p to $\phi(\eta)$ and I verified it manually that it is no longer divisible by higher multiplicities other than one. The divisors are then given by $(2, 5 + \eta_0 + \eta_2 + \eta_5)$ and its cyclic permutations.

After doing Problem 3 using the Python script below I found that $\phi(\eta)$ is actually divisible only 9 times not infinitely many times :)

Page 142, Problem 3. We need to do the same thing as Problem 2 but this time with $\lambda = 23$ and $p = 47$. So this time I wrote a Python script, first to find $\Psi(\eta)$ and then to find $\phi(\eta)$ and check what the multiplicity is for $\phi(\eta)$, if it's more than one then we add p to it and it obviously finds the u's as well.

```
def findOrder(L, p):
    for i in xrange(1,L):
        if pow(p,i,L) == 1:
            return i

def isZeroModP(f, p):
    L = len(f)
    c = f[0] % p
    for k in xrange(1,L):
        if (f[k] % p) != c:
            return False

    return True

def changeModP(f, p):
    L = len(f)
    for i in xrange(L):
        f[i] = f[i] % p

    return f

def checkMultiplicity(f, Psi, p):
    L = len(f)

    res = multCyc(f, Psi)
    mult = 1
    if isZeroModP(res, p) == False:
        return 0
    else:
        for i in xrange(1, 10):
            res = multCyc(res, Psi)
            if isZeroModP(res, pow(p, i + 1)) == False:
                mult = i
                break
        else:
            mult = float('inf')

    return mult

def findPsi(L, p):

    f = findOrder(L, p)
    e = (L - 1)/f

    print 'f =', f

    eta = generateEtas(L, f)
```

```
nz = findEtaNz(eta)

# u is the u in \eta_i \equib u_i
u = [0] * e

Psi = [0] * L
Psi[0] = 1

for v in xrange(p):
    for i in xrange(e):

        t = [1*k for k in eta[i]]
        t[0] -= v
        tmp = [1*k for k in Psi]
        tmp = changeModP(multCyc(tmp, t), p)

        if isZeroModP(tmp, p) == False:
            Psi = [1*k for k in tmp]
        else:
            u[i] = v

# check consistency and print output
etj = [i for i in eta]

# this is the phi from Page 140
phi = [0] * L
g = primRoots(L)[0]
for k in xrange(e):

    # check consistency
    for i in xrange(e):
        etj[i][0] = -u[(i-k) % e]
        tmp = multCyc(Psi, etj[i])
        if isZeroModP(tmp, p) == False:
            print 'There is something wrong', tmp, k, i

    Psi = cycShift(Psi, g)
    # we don't add Psi itself, only its conjugates
    if k < e-1:
        phi = addCyc(phi, Psi)

# we now check how many times phi is divisible
# by this prime factor

mult = checkMultiplicity(phi, Psi, p)

if mult == 0:
    print u'Something wrong with \u03C6(\u03B7)'
elif mult != float('inf'):
    print u'\n\u03C6(\u03B7) is divisible %d times\n' % mult
else:
    print u'is still divisible at 11 multiplicities'


# print output
print u'\u03A8(\u03B7) =',
printSumEtaRaw(Psi, nz)
print
```

```
if mult > 1:
    phi[0] += p
print u'\u03C6(\u03B7) =',
printSumEtaRaw(phi, nz)
print

# something extra check multiplicities of eta_i - u_i
for i in xrange(e):
    eta[i][0] = -u[i]
    mult = checkMultiplicity(eta[i], Psi, p)
    print u'multiplicity of \u03B7%d - %d is %d' % (i, u[i], mult)

return Psi, u
```

The result is that $\psi(\eta)$ is divisible by the prime divisor only once so we get $\psi(\eta)$ immediately

$$\psi(\eta) = \phi(\eta) = 569\eta_0 + 590\eta_1 + 594\eta_2 + 572\eta_3 + 582\eta_4 + 584\eta_5 + 600\eta_6 + 587\eta_7 + 580\eta_8 + 575\eta_9 + 570\eta_{10} + 583\eta_{11} + 574\eta_{12} + 593\eta_{13} + 598\eta_{14} + 578\eta_{15} + 608\eta_{16} + 591\eta_{17} + 602\eta_{18} + 573\eta_{19} + 603\eta_{20} + 567\eta_{21} + 945$$

So the prime divisors are given by $(47, \psi(\eta))$ and its cyclic permutations.

Page 142, Problem 4. We need to find necessary and sufficient condition for "factorization" of $p \neq \lambda$ to be $(p) = (p, \eta_1 - u)(p, \eta_2 - u) \dots (p, \eta_{e-1} - u)$.

The necessary condition is as follows. If we ca factorize $(p) = (p, \eta_1 - u)(p, \eta_2 - u) \dots (p, \eta_{e-1} - u)$ then for some i we have $\eta_i - u \to (\eta_i - u)\Psi(\eta) \equiv 0 \mod p$ according Theorems and Proposition of Section 4.9. Therefore $u \equiv u_i \mod p$ of u_i of Proposition of Section 4.9 and therefore $u = u_i + kp$. If $k \equiv 0 \mod p$ then we might have $\eta_i - u$ divisible multiple times by a prime divisor, to guarantee that it is divisible only once we must have $k \not\equiv 0 \mod p$.

The sufficient condition is also the same, if $u = u_i + kp$ with $k \not\equiv 0 \mod p$ then we can factorize $(p) = (p, \eta_1 - u)(p, \eta_2 - u) \dots (p, \eta_{e-1} - u)$ thanks again to the Proposition and Theorems of Section 4.9.

Page 142, Problem 5. Note that here we are not trying to find an integer v_i such that $(\eta_i - v_i)\Psi^2(\eta) \equiv 0 \mod p$, *i.e.* we are not trying to find $\eta_i \equiv v_i \mod h^\mu(\alpha)$ where $h(\alpha)$ is a prime divisor of p. This was what I was trying to do at first because A now contains multiples of prime divisors.

We are just trying to see what the implication is of having something mod A. So say $f(\alpha) \equiv 0 \mod A$ we can then imply that

$$f(\alpha)w(\alpha) \equiv 0 \mod n$$

where $w(\alpha)$ is such that each $(p_i, \psi_i)^{\mu_i}$ in A becomes p^{μ_i}, *i.e.* $w(\alpha)$ contains all prime divisors of p_i missing from A with the same multiplicity as the one in A.

Now suppose after we found n incongruent cyclotomic integers mod A we find a new one $b(\alpha)$ that is incongruent to all n cyclotomic integers then it must be that

$$\begin{aligned} b(\alpha) - y(\alpha) &\not\equiv 0 \mod A \\ (b(\alpha) - y(\alpha))w(\alpha) &\not\equiv 0 \mod n \\ \rightarrow b(\alpha)w(\alpha) &\not\equiv y(\alpha)w(\alpha) \mod n \end{aligned}$$

where $y(\alpha)$ is any of the n cyclotomic integers we've found so far. But this can't be because mod n means the coefficients of the cyclotomic integer takes the value from 0 to $n-1$ since we've found all cyclotomic integers such that $f(\alpha)w(\alpha)$ has the coefficients between 0 and $n-1$, $b(\alpha)w(\alpha)$ must be one of the ones we've found and in that case $f(\alpha)w(\alpha) \equiv b(\alpha)w(\alpha) \mod n = Aw(\alpha) \rightarrow f(\alpha) \equiv b(\alpha) \mod A$. So there at most can be n incongruent cyclotomic integers mod A, there can be less of course.

Page 142, Problem 6. This is actually quite different from Theorem on Page 140. The norm $N\psi(\eta)$ is not p^f but it's divisible by p^f. Therefore, the norm can have more than f multiples of some prime divisors of p but not f multiples of all of them.

Let's do one direction at a time. If $\psi(\eta)$ is divisible by exactly one prime factor of p then

$$\begin{aligned} \psi(\eta)\Psi_i(\eta) &\equiv 0 \mod p \\ \rightarrow \sigma^k \{\psi(\eta)\Psi_i(\eta)\} \equiv \psi(\sigma^k\eta)\Psi_{i+k}(\eta) &\equiv 0 \mod p \end{aligned}$$

while the norm is given by

$$N\psi(\eta) = \{\sigma\psi(\eta) \cdot \sigma^2\psi(\eta) \cdot \cdots \cdot \sigma^{e-1}\psi(\eta)\}^f$$

The norm is like this because $\psi(\eta)$ is made up of periods with length f where f is the exponent of p mod λ thus $\sigma^e\eta = \eta$ and we can group the norm after every σ^e. From the

equivalence above, we know that $\sigma^k\psi(\eta)$ is "divisible" by $\Psi_{i+k}(\eta)$ which is a conjugate of the prime divisor in question. And since $\psi(\eta)$ doesn't contain any other prime divisor of p its conjugate won't either. To see this, assume we have $\psi(\sigma^k\eta)\Psi_m(\eta) \equiv 0$ and $\psi(\sigma^k\eta)\Psi_n(\eta) \equiv 0$ where $m \neq n$. Conjugating by σ^{e-k} we have $\psi(\sigma\eta)\Psi_{m-k}(\eta) \equiv 0$ and $\psi(\eta)\Psi_{n-k}(\eta) \equiv 0$ which means that our original $\psi(\eta)$ is divisible by more than one prime divisor, a contradiction.

Thus the multiplicity in $N\psi(\eta)$ for each prime divisor of p is f and therefore it is divisible by p^f.

The converse can be solved using the proof of Theorem on Page 140 with slight modification. Let $N\psi(\eta) = b$, from the definition of the norm we have the multiplicity of each prime divisor in $N\psi(\eta)$ to be exactly $(\nu_1 + \nu_2 + \cdots + \nu_e)f$. But since this norm is not equal to p^f, only divisible, the multiplicity of each prime divisor in b can be $f + \Delta$ except for at lest one of them because b is not divisible by p^{f+1}.

So for that particular one we still have $(\nu_1 + \nu_2 + \cdots + \nu_e)f = f$ therefore one ν_i must be 1 and the others 0, thus $\psi(\eta)$ is divisible by exactly one prime divisor of p.

Page 151, Problem 2. Here we need to show that if there is a prime divisor that is not the divisor of a cyclotomic integer then there is a cyclotomic integer that is not divisible by any prime cyclotomic integer.

The hint tells us the answer for this one. The answer is the small $\psi(\eta)$ which is divisible only by one prime divisor of p and not by any other prime divisors.

The next part of the question asks us to show that there is a cyclotomic integer that can be written in two distinct ways as a product of irreducibles.

First, I needed to clarify what it means by irreducibles. I initially thought that if $g(\alpha)$ is such that $Ng(\alpha) = 47 \cdot 139$ (a product of two prime integers) then $g(\alpha)$ is reducible.

But this is not true, being irreducible just means that when you factorize it (if you can factorize it) the only possible factorization is something times a unit. In the example above if $g(\alpha)$ is reducible then $g(\alpha) = f(\alpha)h(\alpha)$ with $Nf(\alpha) = 47$ and $Nh(\alpha) = 139$ but there's no cyclotomic integer whose norm is 47 (neither there is one with norm of 139) therefore $g(\alpha)$ is irreducible.

Another example is $g(\alpha)$ where $Ng(\alpha) = 47^2$, this is also irreducible because if it's

reducible then $g(\alpha) = f(\alpha)h(\alpha)$ with $Nf(\alpha) = 47$ and $Nh(\alpha) = 47$ but there's no cyclotomic integer whose norm is 47 therefore $g(\alpha)$ is irreducible.

Also all prime factors with norm p^f are irreducible because there is no cyclotomic integer with norm p^n witn $n < f$.

So $\psi(\eta)$ is irreducible because although its norm is not a prime integer $N\psi(\eta) = p^f \cdot Q$, p doesn't have real prime factors, because if $\psi(\eta)$ is reducible than one of the factors would have a norm of p^f but that is no actual cyclotomic integer whose norm is p^f.

To show that there is a cyclotomic integer that can be written as a product of irreducibles in two distinct ways we can use Problem 3 of Page 96. Or we can just express the RHS of $N\psi(\eta) = p^f \cdot Q$ in terms of products of irreducibles.

I initially thought what happened if $N\psi(\eta) = p^f$ or when we express p as a product of irreducibles we have $\psi(\eta)$ and its conjugates? because then there's only one way to write this as a product of irreducibles.

Well, p doesn't have actual prime factors, if $N\psi(\eta) = p^f$ then $\psi(\eta)$ is p's actual prime factor. The converse is also true, if we can factorize p into irreducibles whose norm is p^f then those irreducibles are actual prime factors of p. But here p doesn't have actual prime factors so this thing won't happen.

Another thing is that in normal cases where p has prime factors, say $N(\alpha + 4) = 11$ for $\lambda = 5$, we can't say that here we already have more than one way to express 11 as products of cyclotomic integers. One way is $N(\alpha + 4)$ and the other way is 11 itself. But here 11 is not irreducible because it has prime factors.

But the situation is a bit different if p doesn't have actual prime factors, the expression p^f is a product of irreducibles because there are no cyclotomic integers with norm p^f therefore $N\psi(\eta) = p^f \cdot Q$ gives us two ways of writing $N\psi(\eta)$ as a product of irrreducibles (or course once we finish writing Q as a product of irreducibles).

Proposition 151.0. The norm $N\psi(\eta)$ can have other prime factors besides the one in question. Suppose there are only two prime factors in $N\psi(\eta)$, those of p_1 and p_2, and as assumed above one of the prime factors is non-existent. If the prime factor of p_2 is an actual one, call it $h_2(\alpha)$, then $\psi(\eta)$ is divisible by $h_2(\alpha)$ but if this is the case then $\psi(\eta)/h_2(\alpha)$ is an actual cyclotomic integer which is a contradiction since the prime divisor

of p_1 is non-existent.

The situation is the same if we have more than two prime divisors as long as only one of them is fictitious because once we finished dividing by the actual prime factors we get an actual prime divisor for the fictitious one. But if there are two or more fictitious ones we are ok because even if we finished dividing by the actual ones we are left with a cyclotomic integer that is a product of two or more fictitious prime factors.

Also, as mentioned above the norm $N\psi(\eta)$ can't be p^f because then $\psi(\eta)$ is an actual prime factor of p, therefore the norm $N\psi(\eta)$ can only be

$$N\psi(\eta) = p_1^f p_2^{n_2 f} \dots p_k^{n_k f} \cdot q_1^{m_1 f} q_2^{m_1 f} \dots q_l^{m_l f}$$

The p's are primes with no actual prime factors (p_1 is the one whose prime factor is contained in $\psi(\eta)$ with multiplicity one) while the q's are the primes with actual prime factors. The exponents are all multiples of f because $\psi(\eta)$ is made up of periods of length f and so the norm is of the form A^f and by the fundamental theorem the multiplicities must be the same for both sides.

1. Why the obsession with the prime factorization of prime integers?

   I think the answer to this is that given any cyclotomic integer $f(\alpha)$ the norm is $Nf(\alpha)$ which is a normal integer. And we know that any normal integer is a product of prime integers. And so if the prime integers have prime factors it will definitely divide $f(\alpha)$ in a unique way.

2. Is it possible for a prime integer to have an irreducible factor that is not prime?

   Yes, this is shown in Section 4.4. towards the end he (or rather Kummer) showed that for $\lambda = 23$ we can write certain p as a product of 11 conjugates $h(\alpha^j)$ with the property $h(\alpha) = h(\alpha^{-1})$. These $h(\alpha^j)$ are not prime factors and they are irreducible because their norm is p^2 but there's no cyclotomic integer with norm p.

3. So does it mean that reducible means factorizable?

   Depends on what it means to be factorizable. The general answer is yes but it might not be uniquely factorizable. Again, an example is given at the end of Section 4.4.

Here we have $N(1+\alpha+\alpha^{-2}) = 47 \cdot 139$ but each of the prime integers on the RHS does not have prime factors. So this number is clearly reducible and factorizable (the factorization is given by LHS, *i.e.* the product of the conjugates of $1+\alpha+\alpha^{-2}$).

But it's not uniquely factorizable because in that same Section it was shown that we can write both 47 and 139 as products of 11 conjugates. So there are at least two way to factorize it.

4. In Section 4.9 we are introduced to hypothetical prime factors and how we can test divisibility by these factors, does it mean we can deduce norm or conjugates and other properties of cyclotomic integers of these factors?

   No, what you can do is just test divisibility and congruence relations since these factors do not actually exist you cannot take the norm but there are things we can deduce, say our hypothetical factor is $h(\alpha)$ and $h(\alpha)|f(\alpha)$, we can still say that $Nh(\alpha)|Nf(\alpha)$ because it just means that the conjugates of $h(\alpha)$ divides $Nf(\alpha)$ so we must specify what we mean by $Nh(\alpha)|Nf(\alpha)$ here we just mean that the conjugates of $h(\alpha)$ divide $Nf(\alpha)$.