# Harold Edwards Fermat's last theorem

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: February 25, 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 $1600 \rightarrow q = 40$ or $6561 \rightarrow q = 81$. 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 $\gcd(d, z) = c$

$$d^2 k = z^2$$

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

$$D^2 k = Z^2$$

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

$$d^2 K^2 = z^2$$

$$\rightarrow dK = z$$

2

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

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

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

$$DM + ZN = g$$

3

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 $g = D^2a + Z^2b = DgA' + ZgB'$

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

Now, equating the two Bezouts again

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

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 $\gcd(D^n, Z^m)$

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

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

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

5

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

$$\frac{uv}{2} = \frac{y^2}{4} = k^2$$
$$\rightarrow uv = 2k^2$$

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

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

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 $3y^2 \equiv 0 \pmod 6$, note also that since $x$ is odd it can only be of the form $1, 5 \pmod 6$

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

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 $2^{37} \equiv 1 \pmod{p}$, 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

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

9

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

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

$$= pm_x + pm_y + 2$$

$$= pm_{xy} + 2$$

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 $x$)

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

$$= pm_x + pm_y + 1$$

$$= pm_{xy} + 1$$

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 $Q = (p + qr)/|k|$

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

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

$$QR + P \equiv 0 \pmod{K}$$
$$R \equiv Q^{-1}(-P) \pmod{K}$$

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

$$W \equiv QA + PR \equiv QA + P(Q^{-1}(-P)) \pmod{K}$$
$$W \equiv QA - Q^{-1}P^2 \pmod{K}$$
$$QW \equiv Q^2 A - P^2 \equiv 0 \pmod{K}$$

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 $r^2 - A = s$

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

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

$$P - rQ \equiv 0 \quad (\text{mod } K)$$
$$r \equiv Q^{-1}P \quad (\text{mod } K)$$

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

$$R + r \equiv -Q^{-1}P + Q^{-1}P \quad (\text{mod } K)$$
$$\equiv 0 \quad (\text{mod } K)$$

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.

```python
# 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 everytime 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)
```

```python
# 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

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

16

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

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

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 $r \equiv -q^{-1}p \pmod{k}$.

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

$$P - Qr \equiv 0 \pmod{k}$$
$$P - Q(-q^{-1}p) \equiv 0 \pmod{k}$$
$$qP + Qp \equiv 0 \pmod{k}$$

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, $Pr - QA \equiv 0 \pmod{K}$ and since $K = \pm k$ this is also $Pr - QA \equiv 0 \pmod{k}$

$$Pr - QA \equiv 0 \pmod{k}$$
$$P(-q^{-1}p) - QA \equiv 0 \pmod{k}$$
$$pP + qQA \equiv 0 \pmod{k}$$

17

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

$$1 + x + x^2 + x^3 = (1 + x + x^2) + x^3$$
$$= (1 + x)^2 - x + x^3 = (1 + x)^2 - x(1 - x^2)$$
$$= (1 + x)^2 - x(1 + x)(1 - x)$$
$$= (1 + x)[(1 + x) - x(1 - x)] = (1 + x)[1 + x - x + x^2]$$
$$= (1 + x)(1 + x^2)$$

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

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

18

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

$$A^2 = 1 + x + x^3 + x^3 = (1+x)(1+x^2) = (1+2m+1)(1+(2m+1)^2)$$
$$= 2(m+1)(4m^2 + 4m + 2)$$
$$= 4(m+1)(2m^2 + 2m + 1)$$
$$\rightarrow A^2 = 4(m+1)(m^2 + (m+1)^2)$$

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

$$(m+1) - m = 1 = a^2 - b^2 - 2ab$$
$$1 = (a-b)^2 - 2b^2$$

19

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

$$1 = (a - b)^2 - 2b^2$$
$$= (c^2 + d^2 - 2cd)^2 - 2(2cd)^2$$
$$= (c - d)^4 - 8(cd)^2$$

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

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

making the substitution

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

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

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

20

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 $\mp 1$).

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

$$1 = (a - b)^2 - 2b^2$$
$$= (a - 0)^2 - 2 \cdot 0^2$$
$$\rightarrow 1 = a$$

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

$$m + 1 - m = 1 = 2ab - (a^2 - b^2)$$
$$= 2b^2 - (a - b)^2$$

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

$$1 = 2b^2 - (a - b)^2$$
$$= (2B)^2 - (A^2 - 2B^2)^2$$

21

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

$$8A^4 + 1 = k^2$$
$$8A^4 = k^2 - 1$$
$$= (k - 1)(k + 1)$$
$$\to 8A^4 = n(n + 2)$$

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)

$$\pm 2 = 2C^4 - 2^{4r+2}D^4$$
$$\to \pm 1 = C^4 - 2E^4, \qquad E^4 = 2^{4r}D^4$$

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

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

22

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

$$C + F = 2u \qquad\qquad C - F = 2v$$
$$C = u + v \qquad\qquad F = u - v$$

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

$$2E^4 = (u + v)^4 + (u - v)^4$$
$$2E^4 = 2(u^4 + 6u^2v^2 + v^4)$$
$$E^4 = (u^2 + v^2)^2 + (2uv)^2$$

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

$$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2$$
$$(u^2 - v^2)^2 = (u^2 + v^2)^2 - (2uv)^2$$

multiplying both of them

$$(E^2)^2(u^2 - v^2)^2 = \left[(u^2 + v^2)^2 + (2uv)^2\right]\left[(u^2 + v^2)^2 - (2uv)^2\right]$$
$$\left[(E^2)(u^2 - v^2)\right]^2 = (u^2 + v^2)^4 - (2uv)^4$$

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 $B = \pm 1$

23

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 subtituting $C = u + v$ and $F = u - v$

$$2E^4 = (u + v)^4 - (u - v)^4$$
$$= 8uv(u^2 + v^2)$$
$$\rightarrow E^4 = 4uv(u^2 + v^2)$$

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

$$4uv = H^4$$
$$u^2 + v^2 = I^4$$

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 $k^{\text{th}}$ 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

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

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

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

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

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

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?

$$x_{n+2}^2 - 2y_{n+2}^2 = (6x_{n+1} - x_n)^2 - 2(6y_{n+1} - y_n)^2$$
$$= (6^2 x_{n+1}^2 + x_n^2 - 2x_{n+1}x_n) - 2(6^2 y_{n+1}^2 + y_n^2 - 2y_{n+1}y_n)$$

The somewhat problematic terms here are the crossed ones

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

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

$$x_{n+2}^2 - 2y_{n+2}^2 = (6^2 x_{n+1}^2 + x_n^2 - 2 \cdot 6 x_{n+1}x_n) - 2(6^2 y_{n+1}^2 + y_n^2 - 2 \cdot 6 y_{n+1}y_n)$$
$$= 6^2(x_{n+1}^2 - 2y_{n+1}^2) + (x_n^2 - 2y_n^2) - 12(-1)^n(x_1 x_0 - 2y_1 y_0) - 12 \sum_{i=1}^{n}(-1)^{i+n}6(x^2 - 2y^2)$$
$$= \pm 6^2 \pm 1 - 12(-1)^n(x_1 x_0 - 2y_1 y_0) - 12 \sum_{i=1}^{n}(-1)^{i+n}(\pm 6)$$

the $\pm 6^2$, $\pm 1$ in the middle and the $\pm 6$ in the sum depend on $x^2 - 2y^2 = \pm 1$, the last sum is either $0$ or $\pm 6$ 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

26

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

$$x^2 + (x+1)^2 = y^2$$
$$2x^2 + 2x + 1 = y^2$$
$$(2x+1)^2 - 2x^2 - 2x = y^2$$
$$(2x+1)^2 - 2x^2 - 2x - 1 + 1 = y^2$$
$$(2x+1)^2 - y^2 + 1 = y^2$$
$$\rightarrow (2x+1)^2 - 2y^2 = -1$$

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

27

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?

28

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 $X = -\frac{x}{y}$

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

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

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

29

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 $\alpha$ and the constant offset $c = -2$.

Plugging in $\alpha^3$ in place of $\alpha$ 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 $\alpha$ 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 $(A^2 + 3B^2) \not\equiv 0 \pmod 4$.

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

$$Nf(\alpha) = f(\alpha)f(\alpha^2) = (b_0 + b_1\alpha + b_2\alpha^2)(b_0 + b_1\alpha^2 + b_2\alpha)$$

$$= b_0^2 + b_1^2 + b_2^2 + \alpha(b_0b_1 + b_0b_2 + b_1b_2) + \alpha^2(b_0b_1 + b_0b_2 + b_1b_2)$$

$$= b_0^2 + b_1^2 + b_2^2 + (\alpha + \alpha^2)(b_0b_1 + b_0b_2 + b_1b_2)$$

$$= b_0^2 + b_1^2 + b_2^2 + (-1)(b_0b_1 + b_0b_2 + b_1b_2)$$

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 $\alpha^2$ 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 $0, 1, 3, 4 \pmod 6$. The $0, 4$ (mod 6) cases happen only when $c_{0,1}$ are even so we can redo them using $2, 0 \pmod 4$.

31

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 $c_0 c_1$,

$$c_1 + c_0 = u$$

$$c_1 - c_0 = v$$

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

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

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

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

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 $\alpha^4$ term, $f(\alpha) = b_0 + b_1 \alpha + b_2 \alpha^2 + b_3 \alpha^3$.

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

$$b_0^2 + b_1^2 + b_2^2 + b_3^2 + (\alpha + \alpha^4)(b_0 b_1 + b_1 b_2 + b_2 b_3) + (\alpha^2 + \alpha^3)(b_0 b_3 + b_0 b_2 + b_1 b_3)$$

32

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

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

33

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

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

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

```python
# 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 $\lambda$, $i.e.$

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

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 $\lambda$ 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 $g(\alpha) = f(\alpha)f(\alpha^2)\ldots f(\alpha^{\lambda-1})$ and so we have

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

$$\equiv f(1)f(1)\ldots f(1) \pmod{\lambda}$$

$$\equiv \{f(1)\}^{\lambda-1} \pmod{\lambda}$$

but by Fermat's Little Theorem and the fact that $\lambda$ 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

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

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

$$[Nf](1) = [Nf](\alpha) - \lambda[Nf](\alpha)$$
$$\rightarrow [Nf](1) \equiv [Nf](\alpha) \pmod{\lambda}$$

combining this with our previous result we get

$$[Nf](\alpha) \equiv [Nf](1) \equiv \{f(1)\}^{\lambda-1} \pmod{\lambda}$$
$$\equiv 0 \text{ or } 1 \pmod{\lambda}$$

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 $\alpha$, $1^\lambda = 1$ 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 $f(\alpha)$.

37

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 $\lambda$ is prime the set $\{i, 2i, \ldots, (\lambda - 1)i\}$ is equal to the set of remainders of $\lambda$ 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

$$
f(1) + f(\alpha) + \cdots + f(\alpha^{\lambda-1}) = \lambda b_0
$$
$$
\equiv 0 \pmod{\lambda}
$$

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 $\equiv -f(1) \pmod{\lambda}$ and the RHS is $\equiv -g(1) \pmod{\lambda}$ so we practically have $f(1) \equiv g(1) \pmod{\lambda}$ 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 $\lambda$, 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 $\lambda$ is prime there's an inverse of $j$ such that $ij \equiv 1 \pmod{\lambda}$, 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 $1 \pmod{\lambda}$ but also that every prime factor of $Nf(\alpha)$ is 0 or 1 $\pmod{\lambda}$.

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

$$A\alpha^j + B\alpha^k = \alpha^j(A + B\alpha^k)$$
$$\to N(A\alpha^j + B\alpha^k) = N(\alpha^j) \cdot N(A + B\alpha^k)$$
$$= 1 \cdot N(A + B\alpha)$$

but

$$N(A + B\alpha) = (A + B\alpha)(A + B\alpha^2)\ldots(A + B\alpha^{\lambda-1})$$
$$\to (A + B)N(A + B\alpha) = (A + B)(A + B\alpha)(A + B\alpha^2)\ldots(A + B\alpha^{\lambda-1})$$
$$= A^\lambda + B^\lambda$$

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 $\lambda$ is prime and therefore odd we can factorize

$$(A + B)N(A + B\alpha) = A^\lambda + B^\lambda = (A + B)(A^{\lambda-1} - A^{\lambda-2}B + \cdots + B^{\lambda-1})$$
$$\to N(A + B\alpha) = Nf(\alpha) = A^{\lambda-1} - A^{\lambda-2}B + \cdots + B^{\lambda-1}$$

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

$$A^{\lambda-1} - A^{\lambda-2}B + \cdots + B^{\lambda-1} \equiv 0 \pmod{p}$$

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

$$A^{\lambda-1} \equiv -(-A^{\lambda-2}B + \cdots + B^{\lambda-1}) \pmod{p}$$
$$\to B^{-1}A^{\lambda-1} \equiv -(-A^{\lambda-2}B^{-1}B + \cdots + B^{-1}B^{\lambda-1}) \pmod{p}$$
$$\equiv -(-A^{\lambda-2}(-1) + \cdots + B^{\lambda-2}) \pmod{p}$$

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

$$B^{-1}A^{\lambda-1} \equiv -(-A^{\lambda-2} + \cdots + B^{\lambda-2}) \pmod{p}$$

$$B^{-1}A^{\lambda-1} - A^{\lambda-2} \equiv -(A^{\lambda-3}B + \cdots + B^{\lambda-2}) \pmod{p}$$

$$\rightarrow B^{-2}A^{\lambda-1} - B^{-1}A^{\lambda-2} \equiv -(A^{\lambda-3}B^{-1}B + \cdots + B^{-1}B^{\lambda-2}) \pmod{p}$$

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

$$B^{-(\lambda-1)}A^{\lambda-1} - B^{-(\lambda-2)}A^{\lambda-2} + \cdots + 1 \equiv 0 \pmod{p}$$

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

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

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

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

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

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

$$\rightarrow \lambda \equiv 0 \pmod{p}$$

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

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

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 $p \equiv 0 \pmod{\lambda}$ and as shown above $1 + k^{\lambda} \equiv 0 \pmod{p}$ which means that $k$ cannot be 1.

**Page 87, Problem 10**. We want to show that $\alpha^{\lambda-1}$ is the complex conjugate of $\alpha$. This is straightforward enough. From the definition of complex conjugation and the fact that $\alpha$ 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 $\alpha^j$ 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 $\lambda$ 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 $\lambda$ is prime and a (non-zero) multiple of the unit group of $\lambda$ 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 $f(1) \equiv 0 \pmod{\lambda}$. 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 $\equiv 0 \pmod{\lambda}$.

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

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

while on the other hand

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

which is saying that since there are $\lambda$ $m$'s we can spread them to the $\lambda$ 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 $\lambda$ 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

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

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

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

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 $f(1) \equiv 0 \pmod{\lambda}$ 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 $g(1) \equiv 0 \pmod{\lambda}$ and therefore $0 \equiv f(1) \equiv g(1) \pmod{\lambda}$.

But say $\alpha - 1$ does not divide $f(\alpha)$ which means that it doesn't divide $g(\alpha)$ either, this means that $f(1) \equiv k_f \pmod{\lambda}$ and $g(1) \equiv k_g \pmod{\lambda}$, 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 $f(1) - k_g \equiv 0 \pmod{\lambda}$ but we also have $f(1) - k_f \equiv 0 \pmod{\lambda}$, this means that $0 \equiv f(1) - k_g \equiv f(1) - k_f \pmod{\lambda}$ which also means that $k_g \equiv k_f \pmod{\lambda}$ which lastly means that $f(1) \equiv g(1) \pmod{\lambda}$ since $f(1) \equiv k_f$ and $g(1) \equiv k_g \pmod{\lambda}$.

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 $h(1) = f(1) - g(1) \equiv 0 \pmod{\lambda} \rightarrow f(1) \equiv g(1) \pmod{\lambda}$. 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

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

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

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

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 $\lambda = 5$

$$A = 46\alpha^4 - 95\alpha^3 + 53\alpha^2 + 44\alpha - 39$$

$$B = 77\alpha^4 - 57\alpha^3 - 18\alpha^2 - 76\alpha - 80$$

$$AB = -2925\alpha^4 + 8545\alpha^3 - 16819\alpha^2 + 8112\alpha + 1701$$

$$(AB)/A = -134\alpha^3 - 95\alpha^2 - 153\alpha - 157$$

$$(AB)/B = -141\alpha^3 + 7\alpha^2 - 2\alpha - 85$$

and for $\lambda = 7$ I got

$$A = 27\alpha^6 + 36\alpha^5 + 63\alpha^4 + 35\alpha^3 + 19\alpha^2 - 42\alpha + 46$$

$$B = 36\alpha^6 + 62\alpha^5 + 99\alpha^4 + 80\alpha^3 - 66\alpha^2 - 70\alpha - 91$$

$$AB = -488\alpha^6 - 2258\alpha^5 + 6193\alpha^4 + 15480\alpha^3 + 12523\alpha^2 + 3147\alpha + 8091$$

$$(AB)/A = 26\alpha^5 + 63\alpha^4 + 44\alpha^3 - 102\alpha^2 - 106\alpha + 55$$

$$(AB)/B = 9\alpha^5 + 36\alpha^4 + 8\alpha^3 - 8\alpha^2 - 69\alpha + 19$$

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

$$1 = f(\alpha)g(\alpha) = Nf(\alpha)$$
$$= f(\alpha)f(\alpha^2)f(\alpha^3)\ldots f(\alpha^{\lambda-1})$$
$$\rightarrow g(\alpha) = f(\alpha^2)f(\alpha^3)\ldots f(\alpha^{\lambda-1})$$

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

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

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

**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

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

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 "$h(j) \equiv 1 \pmod{\lambda}$ for $j \not\equiv 1 \pmod{\lambda}$". 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 $A$

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

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

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

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

The next thing we need is "A polynomial $F(X)$ is divisible by $(X - 1)$ (mod $\lambda$) if and only if $F(1) \equiv 0 \pmod{\lambda}$." 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 $F(r) \equiv 0 \pmod{\lambda}$ then

$$F(X) \equiv F(X) - F(r)$$

$$\equiv c_n(X^n - r^n) + c_{n-1}(X^{n-1} - r^{n-1}) + \cdots + c_0(1 - 1)$$

$$F(X) \equiv (X - r)\left\{c_n(X^{n-1} + X^{n-2}r + \cdots + Xr^{n-2} + r^{n-1}) + \right.$$

$$\left. c_{n-1}(X^{n-2} + X^{n-3}r + \cdots + Xr^{n-3} + r^{n-2}) + \cdots + c_1\right\}$$

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 $\lambda$ 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, $f(1) \equiv 0 \pmod{\lambda}$ or $g(1) \equiv 0 \pmod{\lambda}$, and using the theorem $F(X)$ divisible by $X - 1$ if and only if $F(1) \equiv 0 \pmod{\lambda}$ 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 $f(\alpha) \rightarrow f(\alpha) - g(\alpha)$ and $g(\alpha) \rightarrow 0$ 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 $X = \alpha$, $i.e.$

$$al(X)(c_1 X^{\lambda-1} + c_2 X^{\lambda-2} + \cdots + c_\lambda) = f(X)h(X) + r(X)$$

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 $\lambda$ 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 $h(\alpha) \rightarrow f(\alpha)h(\alpha) = 0$ 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

$$h(\alpha) \equiv k(\alpha) \quad (\text{mod } f(\alpha)) \to f(\alpha)u(\alpha) = h(\alpha) - k(\alpha) \to f(\alpha)(-u(\alpha)) = k(\alpha) - h(\alpha)$$

which means that $\to k(\alpha) \equiv h(\alpha) \pmod{f(\alpha)}$. Next, transitivity, $h(\alpha) \equiv k(\alpha)$ and $k(\alpha) \equiv g(\alpha)$ means $h(\alpha) \equiv g(\alpha)$

$$h(\alpha) \equiv k(\alpha) \quad (\text{mod } f(\alpha)) \to h(\alpha) - k(\alpha) = f(\alpha)u(\alpha)$$
$$k(\alpha) \equiv g(\alpha) \quad (\text{mod } f(\alpha)) \to k(\alpha) - g(\alpha) = f(\alpha)v(\alpha)$$

adding the two equalities we get

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

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

$$h_1(\alpha) \equiv k_1(\alpha) \quad (\text{mod } f(\alpha)) \to h_1(\alpha) = k_1(\alpha) + f(\alpha)u(\alpha)$$
$$h_2(\alpha) \equiv k_2(\alpha) \quad (\text{mod } f(\alpha)) \to h_2(\alpha) = k_2(\alpha) + f(\alpha)v(\alpha)$$

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

50

$f$ 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

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

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 $\pm 1$ 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 $f(k) \equiv g(k) \pmod{p}$ we also have $f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)}$ 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 $1 - 1 \equiv 0 \pmod{\lambda}$". I found this logic to be a little faulty. The thing is just because $1 - 1 \equiv 0 \pmod{\lambda}$ 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 $7 - 7 \equiv 0 \pmod{\lambda}$ 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 $\lambda$ 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)

$$f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)} \iff f(k) \equiv g(k) \pmod{p} \iff f(\alpha) \equiv g(\alpha) \pmod{h(\alpha^j)}$$

**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 $h(\alpha^j) \equiv g(\alpha) \pmod{h(\alpha)}$ where $g(\alpha)$ can be anything.

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

And from $f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)} \iff f(k) \equiv g(k) \pmod{p} \iff f(\alpha) \equiv g(\alpha) \pmod{h(\alpha^j)}$ we have $g(\alpha) \equiv 0 \pmod{h(\alpha^j)} \iff g(\alpha) \equiv 0 \pmod{h(\alpha)}$. Finally our

original statement $h(\alpha^j) \equiv g(\alpha) \pmod{h(\alpha)}$ means that $h(\alpha^j) \equiv 0 \pmod{h(\alpha)}$. If we start with $h(\alpha) \equiv g(\alpha) \pmod{h(\alpha^j)}$ we will get the other result $h(\alpha) \equiv 0 \pmod{h(\alpha^j)}$.

**Page 92**, mid of top paragraph. $\alpha^j \equiv k \equiv \alpha^i \pmod{\alpha^j}$, note that in this case from the fact that $\alpha \equiv k \pmod{h(\alpha)}$ we have $\alpha^j \equiv k \pmod{h(\alpha^j)}$ for all $j$. We get $k \equiv \alpha^i \pmod{h(\alpha^j)}$ 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 $\alpha \equiv 1 \pmod{\alpha - 1}$.

**Page 93**, top page, $f(\alpha)g(\alpha) \equiv 0 \pmod{\alpha - 1}, f(1)g(1) \equiv 0 \pmod{\alpha - 1}$, this is because $\alpha \equiv 1 \pmod{\alpha - 1}$ so we can substitute 1 for $\alpha$ 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

$$f(\alpha) = q(\alpha)u(\alpha)\tilde{F}(\alpha)$$
$$= p(\alpha)\tilde{F}(\alpha)$$

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 $\lambda$". 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 $\alpha$ is congruent to 1 (mod $\alpha - 1$)", this is because $\alpha \equiv 1 \pmod{\alpha - 1}$ and thus $\alpha^j \equiv 1^j \equiv 1 \pmod{\alpha - 1}$.

**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 $p \equiv 1 \pmod{\lambda}$ 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 $p \equiv 1 \pmod{\lambda}$ 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 $p \equiv 1 \pmod{\lambda}$, 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 $p \equiv 1 \pmod{\lambda}$, 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 $\alpha \equiv k \pmod{h(\alpha)}$, meaning $k^\lambda \equiv 1 \pmod{p^n}$. Now here comes the catch, unlike what happens in the book $k^\lambda - 1$ need not be 0 $\pmod{p^n}$, say it is $p^r \pmod{p^n}$, $r < n$, then Bezout gives us $p^r = a(k^\lambda - 1) + bp^n$ since $Nh(\alpha) = p^n \to h(\alpha)|p^n$ and $1 \equiv \alpha^\lambda \equiv k^\lambda \pmod{h(\alpha)}$ 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 $k^\lambda - 1 \equiv 0 \pmod{p^n}$. We might miss some other $k$'s but that's okay. The next steps would be similar. Again,

54

assume $p \equiv 1 \pmod{\lambda}$.

Let $\gamma$ 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 $(\gamma^i)^\lambda \equiv 1 \pmod{p^n}$ 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

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

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

The proof of the lemma is similar

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

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 $m^\lambda \equiv 1 \pmod{p^n}$ because $m = \gamma^\mu \not\equiv 1 \pmod{p^n}$ since $\gamma$ 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

$$h(X) = q(X)(X - m^j) + r$$
$$h(m^j) = p^n = q(m^j) \cdot 0 + r$$

thus $r \equiv 0 \pmod{p^n}$. Then

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

and the key is that

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

again, since $j = 1, 2, \ldots, \lambda - 1$, $m^j \not\equiv 1 \pmod{p^n}$ and $m^{j\lambda} \equiv \gamma^{j\mu\lambda} \equiv 1 \pmod{p^n}$ 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 $f(\alpha)g(\alpha) \equiv 0 \pmod{h(\alpha)}$ then $f(k)g(k) \equiv 0 \pmod{p^n}$ and vice versa. Even if we can establish that fact $f(k)g(k) \equiv 0 \pmod{p^n}$ still doesn't say that $f(k) \equiv 0 \pmod{p^n}$ or $g(k) \equiv 0 \pmod{p^n}$ 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.* $f(\alpha)g(\alpha) \equiv 0 \pmod{h(\alpha)} \rightarrow f(k)g(k) \equiv 0 \pmod{p}$ 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 $m^\lambda \equiv 1 \pmod{p}$ and $m \not\equiv 1$ $\pmod{p}$". Note that $m = \gamma^\mu$ where $\gamma$ 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 $m = \gamma^\mu$, $\gamma$ a primitive root and $\mu\lambda = p - 1$ thus $m = \gamma^\mu \not\equiv 1$. But $m^j$ can still be one, however, here $j = 1, 2, \ldots, \lambda - 1$ ($\lambda$ 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

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

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

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

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

$$(x+y)N(x+\alpha y) = (x+y)(x+\alpha y)(x+\alpha^2 y)\ldots(x+\alpha^{\lambda-1}y)$$
$$= x^\lambda + y^\lambda$$

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

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

And for $\lambda = 7$

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

And I calculated all these by hand :)

**Page 96, Problem 5**. Show that if a prime $p$ divides $N(x + \alpha y)$ then $p \equiv 1 \pmod{\lambda}$ 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 $N(x + \alpha y) \equiv 0 \pmod{p}$. We then factorize

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

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

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

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

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

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

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

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

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

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 $p \equiv 0 \pmod{\lambda}$ and as shown above $1 + k^\lambda \equiv 0 \pmod{p}$ 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 $p \equiv 1 \pmod{\lambda}$ 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 $\equiv 0 \pmod{p}$. So we don't want $x + y$ to be $0 \pmod{p}$ obviously. Thus

$$x^\lambda + y^\lambda \equiv 0 \pmod{p}$$
$$x^\lambda \equiv -y^\lambda \pmod{p}$$
$$\left(\frac{x}{-y}\right)^\lambda \equiv 1 \pmod{p}$$

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

$$\gamma^\mu \equiv \frac{x}{-y} \pmod{p}$$
$$\to (-y)\gamma^\mu \equiv x \pmod{p}$$

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

$$x + y \equiv y(1 - \gamma^\mu) \pmod{p}$$

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

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

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 $\alpha$,

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

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 $\lambda$.

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 $H(\alpha^j)H(\alpha^k) \equiv 0 \pmod{p}$. 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 $j \not\equiv k \pmod{p}$ then there's an $i \not\equiv 1, 0 \pmod{p}$ such that $ji \equiv k \pmod{p}$ 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

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

$$= \lambda(A_n - A_{n-1})$$

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 $A_{-5} = A_{\lambda-5 \ (\text{mod } \lambda)}$. Therefore since the cross terms $H(\alpha^j)H(\alpha^k) \equiv 0$ for $j \not\equiv k$ we have

$$F^2(n) \equiv \alpha^{-2n}(1-\alpha)^2 H^2(\alpha) + \alpha^{-4n}(1-\alpha^2)^2 H^2(\alpha^2) + \cdots +$$

$$\alpha^{-2(\lambda-1)n}(1-\alpha^{\lambda-1})^2 H^2(\alpha^{\lambda-1})$$

$$F(n+1)F(n-1) \equiv \alpha^{-2n}(1-\alpha)^2 H^2(\alpha) + \alpha^{-4n}(1-\alpha^2)^2 H^2(\alpha^2) + \cdots +$$

$$\alpha^{-2(\lambda-1)n}(1-\alpha^{\lambda-1})^2 H^2(\alpha^{\lambda-1})$$

Thus

$$F^2(n) - F(n+1)F(n-1) \equiv 0 \equiv \lambda^2(A_n - A_{n-1})^2 - \lambda^2(A_{n+1} - A_n)(A_{n-1} - A_{n-2}) \quad (\text{mod } p)$$

$$\rightarrow \frac{(A_n - A_{n-1})}{(A_{n+1} - A_n)} \equiv \frac{(A_{n-1} - A_{n-2})}{(A_n - A_{n-1})} \quad (\text{mod } p)$$

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 $\xi \equiv \frac{(A_n - A_{n-1})}{(A_{n+1} - A_n)}$, $\xi$ must be independent of $n$. To see this, start with $F^2(2) - F(3)F(1) \equiv 0$ to get

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

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

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

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 $F^2(-1) \equiv \lambda^2(A_{-1 \equiv \lambda-1 \ (\text{mod } \lambda)} - A_{-2 \equiv \lambda-2 \ (\text{mod } \lambda)})^2$, therefore if any of the differences is zero then all of them will be zero which means that $A_0 = A_1 = A_2 = \cdots = A_{\lambda-1}$

63

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 $\xi$ is well defined.

Now, if we rewrite the identity

$$\frac{(A_n - A_{n-1})}{(A_{n+1} - A_n)} \equiv \frac{(A_{n-1} - A_{n-2})}{(A_n - A_{n-1})} \rightarrow (A_n - A_{n-1}) \equiv (A_{n+1} - A_n)\frac{(A_{n-1} - A_{n-2})}{(A_n - A_{n-1})}$$
$$\rightarrow (A_n - A_{n-1}) \equiv (A_{n+1} - A_n)\xi$$
$$\rightarrow \xi A_n - A_{n-1} \equiv \xi A_{n+1} - A_n$$

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 $(\alpha - \xi)H(\alpha) \equiv 0 \pmod{p}$

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

because the terms in brackets is the usual zero. Thus $(\alpha - \xi)H(\alpha) \equiv 0 \pmod{p}$ 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 $p \equiv 1 \pmod{\lambda}$ is divisible by prime $h(\alpha)$ then there are precisely $\lambda - 1$ solutions to $k^\lambda \equiv 1 \pmod{\lambda}$ with $k \not\equiv 1 \pmod{\lambda}$.

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 $f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)} \iff f(k) \equiv g(k) \pmod{p}$. From page 92 we know that

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

which also means that $k^\lambda - 1 = (k-1)(k^{\lambda-1} + k^{\lambda-2} + \cdots + k + 1) \equiv 0 \pmod{p}$. 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 $f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)} \iff f(k) \equiv g(k) \pmod{p}$ then

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

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

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 $p \equiv 1 \pmod{\lambda}$ 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 $\lambda$ so it at most has $\lambda$ 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 $\lambda$ roots.

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

According to Theorem on Page 91, this means that $k = 7$ where $\alpha \equiv k \pmod{h(\alpha)}$. 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 $\alpha \equiv 7 \pmod{\alpha - 7}$. 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 $k^{\lambda-1} + k^{\lambda-2} + \cdots + 1 \equiv 0 \pmod{p}$ then $f(\alpha) = g(\alpha)$ implies $f(k) \equiv g(k) \pmod{p}$.

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

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

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

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

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 $f(k) - g(k) = q(k)(k^{\lambda-1} + k^{\lambda-2} + \cdots + 1) \equiv 0 \pmod{p} \to f(k) \equiv g(k) \pmod{p}$ since the problem tells us that $k^{\lambda-1} + k^{\lambda-2} + \cdots + 1 \equiv 0 \pmod{p}$.

**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 $g(-2) \equiv 0 \pmod{11}$. This comes from Theorem of Page 91, $f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)} \iff f(k) \equiv g(k) \pmod{p}$.

66

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 $\alpha + 2 \equiv 0 \pmod{h(\alpha)}$, a trivial identity, we therefore have $\alpha \equiv -2 \pmod{h(\alpha)}$, $k = -2$ and $p = Nh(\alpha) = 11$ therefore Theorem on Page 91 gives us

$$g(\alpha) \equiv (\alpha + 2)y(\alpha) \pmod{h(\alpha)} \Longleftrightarrow g(-2) \equiv (-2+2)y(-2) \equiv 0 \pmod{11}$$

**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

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

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

**Page 100**. Top page, we started the guess of $g(-13) \equiv 0 \pmod{29}$ 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 $k + 4 \equiv 0 \pmod{29}$, 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 $(-13)^4 \equiv -4 \pmod{29}$ 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, "$N(\alpha - 4) \equiv 0 \pmod{47}$". This is because $N(\alpha - 4) = \frac{1^{23} - 4^{23}}{1 - 4}$ but $4^{23} = 2^{2 \cdot 23} \equiv 2^{47-1} \equiv 1 \pmod{47}$.

**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 $(3 - \alpha)$

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

**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 $(\alpha^2 + 2)$. From

$$\alpha^2 \equiv -2 \pmod{\alpha^2 + 2}$$
$$\rightarrow k^2 \equiv -2 \pmod{11}$$

and the fact that $1 \equiv \alpha^{\lambda = 5} \equiv k^5 \rightarrow k^6 \equiv k$ we know that $k^6 \equiv (-2)^3 \equiv 3 \pmod{11}$. So $\alpha \equiv 3 \pmod{\alpha^2 + 2}$ therefore it is $3 - \alpha$ itself that is divisible by $\alpha^2 + 2$. But substituting $\alpha \rightarrow 3$ in the other conjugates $3 - \alpha^j$ doesn't product $0 \pmod{11}$ and there are two counts of $\alpha^2 + 2$ in the RHS above, therefore both $\alpha^2 + 2$ 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 $f(\alpha)g(\alpha) = h(\alpha) \rightarrow g(\alpha) = \frac{h(\alpha)f(\alpha^2)f(\alpha^3)...f(\alpha^{\lambda-1})}{Nf(\alpha)}$, 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

$$\frac{(3 - \alpha)\{(\alpha + 2)(\alpha^3 + 2)(\alpha^4 + 2)\}^2}{11^2} = \frac{\not{11}(\alpha^4 + \alpha^3 + 4)(\alpha + 2)(\alpha^3 + 2)(\alpha^4 + 2)}{11^{\not{2}}}$$
$$= \frac{(\alpha^4 + \alpha^3 + 4)(\alpha + 2)(\alpha^3 + 2)(\alpha^4 + 2)}{(\alpha + 2)(\alpha^2 + 2)(\alpha^3 + 2)(\alpha^4 + 2)}$$
$$= \frac{(\alpha^4 + \alpha^3 + 4)}{(\alpha^2 + 2)}$$

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

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

Therefore

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

69

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

For $\alpha^2 + 2$ we have $k^2 \equiv -2 \to k^6 \equiv 3$ (mod 11) therefore $5 + 2\alpha \to 5 + 6 = 11$ and therefore $5 + 2\alpha$ is divisible by $\alpha^2 + 2$. 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 $\alpha \to 49$ 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, $\alpha^3 + 2$ means that $k^3 \equiv -2$ and $k \equiv k^6 = (-2)^2 \equiv 4$ (mod 11) therefore $\alpha + 7 \to 4 + 7 = 11 \equiv 0$ (mod 11) and $\alpha + 7$ is divisible by $\alpha^3 + 2$.

From Page 98 we know that $k \equiv 49$ for $2\alpha^4 + \alpha^2 + 4$, conjugating $\alpha \to \alpha^2$ 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 $\alpha + 7 \to -7 + 7 \equiv 0$ (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 $\alpha^4 - 5 \to 16 - 5 = 11 \equiv 0$ (mod 11) and therefore $\alpha + 2$ divides $\alpha^4 - 5$.

**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 $k^2 \equiv -34 \rightarrow k^8 \equiv k \equiv 45$ (mod 71) causing $2k^5 + 2k^2 + k + 1 \equiv 3$ (mod 71) a no go.

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

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

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

For $3 - 2\alpha^6$ we have $k^6 \equiv -34 \rightarrow k^{36} \equiv k \equiv 48$ (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 $N(1 + \alpha^2 - \alpha^4) = 29$)

$$\alpha \to \alpha^2 \to 1 + k^4 - k \equiv 0 \pmod{29}$$
$$\alpha \to \alpha^3 \to 1 + k^6 - k^5 \equiv -12 \pmod{29}$$
$$\alpha \to \alpha^4 \to 1 + k - k^2 \equiv -19 \pmod{29}$$
$$\alpha \to \alpha^5 \to 1 + k^3 - k^6 \equiv 15 \pmod{29}$$
$$\alpha \to \alpha^6 \to 1 + k^5 - k^3 \equiv -2 \pmod{29}$$

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 $\lambda$ and find $e$ and $f$ that minimizes $e + f$ where $ef = \lambda - 1$ this is because

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

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 $\alpha^6 - 2\alpha^3 + \alpha + 1$.

74

It turned out that $3 - \alpha^6 - \alpha^2 \to 3 - 6^6 - 6^2 \equiv 0 \pmod{197}$. 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 $5 - 3 - 5 + 5 - 2 \equiv 0 \pmod 5$. 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 $F(\alpha) = f(\alpha) \cdot \sigma^2 f(\alpha) \cdot \sigma^4 f(\alpha) \cdot \sigma^6 f(\alpha) \cdots \sigma^{16} f(\alpha) = a + b\theta_0$ 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 $\lambda$ :) 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

$$f(\alpha) = a_0 + a_1(\alpha + \alpha^{-1}) + a_2(\alpha^2 + \alpha^{-2}) + \cdots + a_{11}(\alpha^{11} + \alpha^{-11})$$

78

setting $\alpha \to 4$ 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 $f(\alpha) \equiv 0 \pmod{47}$ 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 $\alpha$ 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 \pmod{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 $f(4) \equiv 0 \pmod{47}$.

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

$$f(\alpha) = -(\alpha^1 + \alpha^{-1}) + (\alpha^3 + \alpha^{-3}) + (\alpha^9 + \alpha^{-9})$$

$$\rightarrow f(4) \equiv -16 + 6 + 10 \equiv 0 \pmod{47}$$

but the questions asks for a few solutions so here are a couple more

$$f(\alpha) = 2 - (\alpha^2 + \alpha^{-2}) + (\alpha^5 + \alpha^{-5}) + (\alpha^{10} + \alpha^{-10})$$

$$f(\alpha) = -(\alpha^2 + \alpha^{-2}) + (\alpha^8 + \alpha^{-8}) + (\alpha^{10} + \alpha^{-10})$$

As noted earlier Kummer's solution satisfies $f(4) \equiv 0 \pmod{47}$ 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 $\lambda$ 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 $\lambda$ is prime there must be an integer $i$ such that $ij \equiv 1 \pmod{\lambda}$, 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

$$(1 - 2)\alpha + (2 - 3)\alpha^2 + \cdots + (\lambda - 1 - \lambda)\alpha^{\lambda - 1} + \lambda - 1 = \lambda - 1 - (\alpha + \alpha^2 + \cdots + \alpha^{\lambda - 1})$$

$$= \lambda - 1 + 1 = \lambda$$

80

The harder way is to do long division on $N(\alpha-1)$ by $\alpha-1$ to get $(\alpha^2-1)(\alpha^3-1)\ldots(\alpha^{\lambda-1}-1)$. But first we need to massage $N(\alpha-1) = \lambda \to \alpha^{\lambda-1} + \alpha^{\lambda-2} + \cdots + (1+\lambda)$.

$$
\begin{array}{r}
\alpha^{\lambda-2} + 2\alpha^{\lambda-3} + 3\alpha^{\lambda-4} + 4\alpha^{\lambda-5} + \quad \cdots \quad + (\lambda-1) \\
\hline
\alpha - 1 \; \sqrt{\alpha^{\lambda-1} + \alpha^{\lambda-2} + \alpha^{\lambda-3} + \alpha^{\lambda-4} + \alpha^{\lambda-5} + \quad \cdots \quad + (1+\lambda)} \\
\alpha^{\lambda-1} - \alpha^{\lambda-2} \\
\hline
2\alpha^{\lambda-2} + \alpha^{\lambda-3} \\
2\alpha^{\lambda-2} - 2\alpha^{\lambda-3} \\
\hline
3\alpha^{\lambda-3} + \alpha^{\lambda-4} \\
3\alpha^{\lambda-3} - 3\alpha^{\lambda-4} \\
\hline
4\alpha^{\lambda-4} + \alpha^{\lambda-5} \\
4\alpha^{\lambda-4} - 4\alpha^{\lambda-5} \\
\hline
\vdots \\
\hline
(\lambda-1)\alpha + (\lambda+1) \\
(\lambda-1)\alpha - (\lambda-1) \\
\hline
2\lambda
\end{array}
$$

Therefore

$$
\frac{\lambda}{\alpha-1} = \alpha^{\lambda-2} + 2\alpha^{\lambda-3} + 3\alpha^{\lambda-4} + 4\alpha^{\lambda-5} + \cdots + (\lambda-1) + \frac{2\lambda}{\alpha-1}
$$

$$
\to \frac{\lambda}{\alpha-1} = -\alpha^{\lambda-2} - 2\alpha^{\lambda-3} - 3\alpha^{\lambda-4} - 4\alpha^{\lambda-5} - \cdots - (\lambda-1)
$$

$$
= \lambda\alpha^{\lambda-1} + (\lambda-1)\alpha^{\lambda-2} + (\lambda-2)\alpha^{\lambda-3} + (\lambda-3)\alpha^{\lambda-4} + (\lambda-4)\alpha^{\lambda-5} + \ldots 1
$$

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 $\sigma$ 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 $\alpha$ 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, $\eta_i$, is made of repeated applications of $\sigma$, *i.e.* to create a period take a power of alpha, $\alpha^j$, 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 $\eta_0$ we have to start with $\alpha$ we can start with any $\alpha^j$ but it must contain $\alpha$ at the end so it's easier to start with $\alpha$.

**Page 109**. Top page, proof that periods are independent of the choice of primitive roots. First it says "if $\alpha^j$ is any power of $\alpha$, and if $\eta_i$ is the period which contains it, then $\eta_i$ also contains $\sigma'^e \alpha^j$. (Then it also contains $\sigma'^e \sigma'^e \alpha^j = \sigma'^{2e} \alpha^j, \sigma'^{3e} \alpha^j, \dots, \sigma'^{-e} \alpha^j$".

The note in bracket is just the consequence of the previous if, what it says is first we need to establish that if $\alpha^j$ is in $\eta_i$ then $\sigma^e \alpha^j$ is also in $\eta_i$. Once this is established we note that $\sigma^e \alpha^j$ is just $\alpha^k$ for some $k$ but by the application of the if statement $\alpha^k$ in $\eta_i$ means that $\sigma^e \alpha^k = \sigma^{2e} \alpha^j$ is also in $\eta_i$ and we can repeat the argument again and again.

**Page 109**. Top page, continuation of the above proof, "suffice to prove that $\sigma'^e$ is a power of $\sigma^e$". To see this, the first key is to note that any period can be expressed as sums of powers of $\sigma^e$ with the appropriate choice of $\alpha^j$

$$\eta_i = \alpha^j + \sigma^e \alpha^j + \sigma^{2e} \alpha^j + \cdots + \sigma^{-e} \alpha^j$$
$$= \sum_{s=0}^{f-1} \sigma^{se} \alpha^j$$

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 $\sigma^{me}$ is one of those $\sigma^{se}$? Easy, this is because $\sigma^{efn} = 1$ so we just need $m \pmod{f}$, let $l \equiv m \pmod{f}$ then $\sigma^{me} = \sigma^{le}$ with $0 \le l < f$ but $s$ runs from $0 \le s < f$ thus we are guaranteed to find a value of $s$ such that $s \equiv m \pmod{f}$.

**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 $\theta_0$ and $\theta_1$

$$\theta_0 = \alpha + \sigma^2 \alpha = \alpha + \alpha^4$$
$$\theta_1 = \sigma \theta_0 = \alpha^2 + \alpha^3$$

The multiplication table is

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

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 $\theta_1$ 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 $\not\equiv 0, 1 \pmod 5$ 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 $\not\equiv 0, 1 \pmod 5$ :)

From Page 96, Problem 5, if $p$ divides the norm of a binomial then $p \equiv 0, 1 \pmod \lambda$, 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 $\theta_0$ and $\theta_1$. In which case the period length is $f = 3$.

If this is the case then the norm is given by

$$Nf(\alpha) = (a\theta_0 + b\theta_1)(a\theta_1 + b\theta_0)$$
$$= (a^2 + b^2)\theta_0\theta_1 + ab(\theta_0^2 + \theta_1^2)$$

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

$$\theta_0 = \alpha + \alpha^{3^2} + \alpha^{3^4}$$
$$= \alpha + \alpha^2 + \alpha^4$$
$$\theta_1 = \alpha^3 + \alpha^5 + \alpha^6$$
$$\theta_0\theta_1 = 3 + \theta_0 + \theta_1$$
$$= 2$$

83

and also

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

since $\theta_0 + \theta_1 = -1$. Thus

$$Nf(\alpha) = 2a^2 - 3ab + 2b^2$$

Let $a + b = u, a - b = v$ and

$$2a^2 - 3ab + 2b^2 = \tfrac{1}{4}\{2(u+v)^2 - 3(u^2 - v^2) + 2(u-v)^2\}$$
$$= \tfrac{1}{4}\{u^2 + 7v^2\}$$

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 $\tfrac{1}{4}(2u^2 - 2uv + 4v^2)$.

**Page 110, Problem 3**. We want to calculate $(\theta_0 - \theta_1)^2$ for several values of $\lambda$,

$$
\begin{array}{llll}
\lambda = 3 & \rightarrow (\theta_0 - \theta_1)^2 = -3 & \frac{\lambda-1}{2} = 1 \\
\lambda = 5 & \rightarrow (\theta_0 - \theta_1)^2 = 5 & \frac{\lambda-1}{2} = 2 \\
\lambda = 7 & \rightarrow (\theta_0 - \theta_1)^2 = -7 & \frac{\lambda-1}{2} = 3 \\
\lambda = 11 & \rightarrow (\theta_0 - \theta_1)^2 = -11 & \frac{\lambda-1}{2} = 5 \\
\lambda = 13 & \rightarrow (\theta_0 - \theta_1)^2 = 13 & \frac{\lambda-1}{2} = 6 \\
\lambda = 17 & \rightarrow (\theta_0 - \theta_1)^2 = 17 & \frac{\lambda-1}{2} = 8 \\
\lambda = 19 & \rightarrow (\theta_0 - \theta_1)^2 = -19 & \frac{\lambda-1}{2} = 9 \\
\lambda = 23 & \rightarrow (\theta_0 - \theta_1)^2 = -23 & \frac{\lambda-1}{2} = 11 \\
\lambda = 29 & \rightarrow (\theta_0 - \theta_1)^2 = 29 & \frac{\lambda-1}{2} = 14 \\
\lambda = 31 & \rightarrow (\theta_0 - \theta_1)^2 = -31 & \frac{\lambda-1}{2} = 15 \\
\end{array}
$$

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 $\sigma^e$ if and only if it is made of periods.

   *Proof.* The only if part is easy, if it's made of periods it's of course invariant under $\sigma^e$. The other way is also easy. To be invariant under $\sigma^e$ means that if any $\alpha^j$ 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 $\theta_i$) 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 $\theta_0$ and get $(\theta_0 - \theta_1)^2 = 4(\theta_1^2 + \theta_1) + 1$.

85

3. No.1 above shows that (as mentioned earlier) we can express

$$\theta_0^2 = a\theta_0 + b\theta_1$$

$$\rightarrow \sigma\theta_0^2 = \theta_1^2 = a\theta_1 + b\theta_0$$

The identity $(\theta_0 - \theta_1)^2 = 4(\theta_0^2 + \theta_0) + 1 = 4(\theta_1^2 + \theta_1) + 1$ gives

$$4(\theta_0^2 + \theta_0) + \cancel{1} = 4(\theta_1^2 + \theta_1) + \cancel{1}$$

$$a\theta_0 + b\theta_1 + \theta_0 = a\theta_1 + b\theta_0 + \theta_1$$

$$\rightarrow [(a+1) - b]\theta_0 = [(a+1) - b]\theta_1$$

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

$$(\theta_0 - \theta_1)^2 = 4(\theta_0^2 + \theta_0) + 1$$

$$= -4(a+1) + 1$$

We now need to find the value of $a$ as a function of $\lambda$.

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 $\theta_0$ and $\theta_1$ in $\theta_0^2$, we know that

$$\theta_0 = \sum_{u=0}^{f-1} \sigma^{ue}\alpha$$

$$\rightarrow \theta_0^2 = \left(\sum_{u=0}^{f-1} \sigma^{ue}\alpha\right)^2$$

$$= \left(\sum_{u=0}^{f-1} \sigma^{ue}\alpha^2\right) + 2 \times \{\text{cross terms}\}$$

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 $\theta_0$ or $\theta_1$ 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 $\lambda$ as $\beta$ 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 $\alpha^\lambda$ we must have

$$\alpha^{\beta^{u_1 e} + \beta^{u_2 e}} = 1$$
$$\to \beta^{u_1 e} + \beta^{u_2 e} \equiv 0 \pmod{\lambda}$$
$$\beta^{u_1 e}(1 + \beta^{(u_2 - u_1)e}) \equiv 0 \pmod{\lambda}$$

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 $\alpha^\lambda$.

The question now is how many of the cross terms are $\alpha^\lambda$? $-1 \equiv \beta^{ke}$ means that $1 \equiv \beta^{2ke}$ but since $\beta$ is a primitive root this means that $2ke = 2f \to k = \frac{f}{2}$ (recall

87

that $e = 2$). Thus the only combinations that produce $\alpha^\lambda$ 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

$$(f - 1) - \frac{f}{2} + 1 = \frac{f}{2}$$

corss terms that produce $\alpha^\lambda$. 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 $\beta^{w_1 e}(1 + \beta^{(w_2 - w_1)e}) \equiv 0 \pmod{\lambda}$ then $-1 \equiv \beta^{(w_2 - w_1)e}$ but since $\beta$ 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

$$2B - 1 = f - 1$$
$$\rightarrow B = \frac{f}{2}$$
$$\rightarrow A = \frac{f}{2} - 1$$

88

and $a = A - C = -\frac{f}{2} - 1$ and

$$(\theta_0 - \theta_1)^2 = -4(a + 1) + 1$$
$$= 2f + 1 = \lambda$$

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 $\alpha^\lambda$ 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

$$(\theta_0 - \theta_1)^2 = -4(a + 1) + 1$$
$$= -2(f + 1) + 1 = -\lambda$$

consistent with the answer to Problem 3.

**Page 110, Problem 5**. We want to find the general formula for $Ng(\alpha)$ for any prime $\lambda$, what we need is the formula from Problem 3 because we need the value of $\theta_0\theta_1$ (to avoid clutter let $r = (-1)^{\frac{\lambda-1}{2}}$)

$$(-1)^2 = (\theta_0 + \theta_1)^2 = \theta_0^2 + \theta_1^2 + 2\theta_0\theta_1$$
$$(-1)^{\frac{\lambda-1}{2}}\lambda = (\theta_0 - \theta_1)^2 = \theta_0^2 + \theta_1^2 - 2\theta_0\theta_1$$
$$\rightarrow \frac{1 - r\lambda}{4} = \theta_0\theta_1$$

and also

$$(-1)^2 = (\theta_0 + \theta_1)^2 = (\theta_0^2 + \theta_1^2) + 2\theta_0\theta_1$$
$$1 = (\theta_0^2 + \theta_1^2) + \frac{1 - (-1)^{\frac{\lambda-1}{2}}\lambda}{2}$$
$$\rightarrow \frac{1 + r\lambda}{2} = (\theta_0^2 + \theta_1^2)$$

89

therefore

$$Ng(\alpha) = (a^2 + b^2)\theta_0\theta_1 + ab(\theta_0^2 + \theta_1^2)$$
$$= (a^2 + b^2)\frac{1 - r\lambda}{4} + ab\frac{1 + r\lambda}{2}$$

Now as usual let $a + b = u$ and $a - b = v$ first let

$$w = \frac{1 - r\lambda}{4}$$
$$t = \frac{1 + r\lambda}{2}$$
$$\to 2w + t = 1$$
$$\to 2w - t = -r\lambda = -(-1)^{\frac{\lambda - 1}{2}}\lambda$$

then

$$Ng(\alpha) = \frac{1}{4}\left\{(2w + t)u^2 + (2w - t)v^2\right\}$$
$$= \frac{1}{4}\left\{u^2 - (-1)^{\frac{\lambda - 1}{2}}\lambda v^2\right\}$$

**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 $\sigma$ powers

$$\sigma^{1\cdot4} \to \alpha^{3^4} = \alpha^{13}$$
$$\sigma^{2\cdot4} \to \alpha^{3^8} = \alpha^{16}$$
$$\sigma^{3\cdot4} \to \alpha^{3^{12}} = \alpha^4$$

therefore the periods are

$$\eta_0 = \alpha + \sigma^e\alpha + \sigma^{2e}\alpha + \sigma^{3e}\alpha$$
$$= \alpha + \alpha^{13} + \alpha^{16} + \alpha^4$$
$$\sigma\eta_0 = \eta_1 = \alpha^3 + \alpha^5 + \alpha^{14} + \alpha^{12}$$
$$\sigma\eta_1 = \eta_2 = \alpha^9 + \alpha^{15} + \alpha^8 + \alpha^2$$
$$\sigma\eta_2 = \eta_3 = \alpha^{10} + \alpha^{11} + \alpha^7 + \alpha^6$$

90

the multiplication table is

$$\eta_0^2 = (\alpha^2 + \alpha^9 + \alpha^{15} + \alpha^8) + 2(\alpha^{14} + 1 + \alpha^5 + \alpha^{12} + 1 + \alpha^3)$$

$$= \eta_2 + 2(\eta_1 + 2)$$

$$= \eta_2 + 2\eta_1 + 4$$

$$\eta_0\eta_1 = 2\eta_0 + \eta_2 + \eta_3$$

$$\eta_0\eta_2 = \eta_0 + \eta_1 + \eta_2 + \eta_3$$

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 $p \equiv \gamma^j \pmod{\lambda}$, 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 $\eta_0$ is independent of the choice of primitive root. We know that $\eta_0$ is the only one that contains $\alpha$ and different primitive roots give the same periods (sans the ordering) therefore $\eta_0$ must be the same since it is the only one with $\alpha$ so that's the short story :)

**Page 113**. Top page, note that what was proven in the previous page is $X^p - X \equiv (X-1)(X-2)\ldots(X-p) \pmod{p}$. However, in this page what we have is $g(\alpha)^p - g(\alpha) \equiv (g(\alpha) - 1)(g(\alpha) - 2)\ldots(g(\alpha) - p) \pmod{p}$. 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 $X^p - X - (X-1)(X-2)\ldots(X-p)$ 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 $g(\alpha)^p - g(\alpha) - (g(\alpha) - 1)(g(\alpha) - 2)\ldots(g(\alpha) - p)$ has the same coefficients they are also $0 \pmod{p}$.

**Page 114, Problem 1**. Here we are computing Pascal triangle up to $n = 13$ and

91

verifying that the coefficients are multiple of $n$ when $n$ is prime

$$
\begin{aligned}
n &= 1 &\to& \ 1 \\
n &= 2 &\to& \ 1\ 2\ 1 \\
n &= 3 &\to& \ 1\ 3\ 3\ 1 \\
n &= 4 &\to& \ 1\ 4\ 6\ 4\ 1 \\
n &= 5 &\to& \ 1\ 5\ 10\ 10\ 5\ 1 \\
n &= 6 &\to& \ 1\ 6\ 15\ 20\ 15\ 6\ 1 \\
n &= 7 &\to& \ 1\ 7\ 21\ 35\ 35\ 21\ 7\ 1 \\
n &= 8 &\to& \ 1\ 8\ 28\ 56\ 70\ 56\ 28\ 8\ 1 \\
n &= 9 &\to& \ 1\ 9\ 36\ 84\ 126\ 126\ 84\ 36\ 9\ 1 \\
n &= 10 &\to& \ 1\ 10\ 45\ 120\ 210\ 252\ 210\ 120\ 45\ 10\ 1 \\
n &= 11 &\to& \ 1\ 11\ 55\ 165\ 330\ 462\ 462\ 330\ 165\ 55\ 11\ 1 \\
n &= 12 &\to& \ 1\ 12\ 66\ 220\ 495\ 792\ 924\ 792\ 495\ 220\ 66\ 12\ 1 \\
n &= 13 &\to& \ 1\ 13\ 78\ 286\ 715\ 1287\ 1716\ 1287\ 715\ 286\ 78\ 13\ 1
\end{aligned}
$$

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 $X(X-1)(X-2)\ldots(X-p+1)$ for $p = 3, 5, 7, 11$.

$$
\begin{aligned}
p &= 3 &\to X\ldots(X-2) &= X^3 - 3X^2 + 2X \\
p &= 5 &\to X\ldots(X-4) &= X^5 - 10X^4 + 35X^3 - 50X^2 + 24X \\
p &= 7 &\to X\ldots(X-6) &= X^7 - 21X^6 + 175X^5 - 735X^4 + 1624X^3 - 1764X^2 + 720X \\
p &= 11 &\to X\ldots(X-10) &= X^{11} - 55X^{10} + 1320X^9 - 18150X^8 + 157773X^7 - 902055X^6 + \\
& & & \quad 3416930X^5 - 8409500X^4 + 12753576X^3 - 10628640X^2 + 3628800X
\end{aligned}
$$

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 $\equiv X^p - X \pmod{p}$.

**Page 114, Problem 3**. We need to verify $\eta^p \equiv \eta \pmod{p}$ 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

92

have $e = 2, f = 3$ or $e = 3, f = 2$. But $\eta^p \equiv \eta$ only works if $\eta$ is a period of length $f$ where $f$ is the exponent (or I rpefer to call it order) of $p \pmod{\lambda}$.

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

$$\eta_0 = \alpha + \alpha^2 + \alpha^4$$
$$\sigma\eta_0 = \eta_1 = \alpha^3 + \alpha^5 + \alpha^6$$

with $p = 2$ we have

$$\eta_0^2 = \alpha^2 + \alpha^4 + \alpha + 2(\alpha^3 + \alpha^5 + \alpha^6)$$
$$= \theta_0 + 2\theta_1$$
$$\equiv \theta_0 \pmod{p}$$
$$\eta_1^2 = \alpha^6 + \alpha^3 + \alpha^5 + 2(\alpha + \alpha^2 + \alpha^4)$$
$$= \eta_1 + 2\eta_0$$
$$\equiv \eta_1 \pmod{p}$$

Now, if we choose $e = 3, f = 2$ where $f$ is no longer the exponent of $p \pmod{\lambda}$ 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

$$\eta_0^2 = \alpha^2 + \alpha^5 + 2 \equiv \eta_2 \pmod{p}$$

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 $p \pmod{\lambda}$) we must have $e = 4$, the primitive roots mod 13 are 2, 6, 7, 11, let's choose 2

$$\eta_0 = \alpha + \alpha^3 + \alpha^9$$
$$\sigma\eta_0 = \eta_1 = \alpha^2 + \alpha^6 + \alpha^5$$
$$\sigma\eta_1 = \eta_2 = \alpha^4 + \alpha^{12} + \alpha^{10}$$
$$\sigma\eta_2 = \eta_3 = \alpha^8 + \alpha^{11} + \alpha^7$$

93

with $p = 3$ we have from the formula $(x + y + z)^4 = x^3 + y^3 + z^3 + 3(yz^2 + xz^2 + y^2z + x^2z + xy^2 + x^2y) + 6xyz$

$$\eta_0^3 = \alpha^3 + \alpha^9 + \alpha + 3(\alpha^5 + \alpha^{11} + \alpha^7 + \alpha^6 + \alpha^2 + \alpha^8) + 6 = \eta_0 + 3(\eta_1 + \eta_3) + 6$$

$$\equiv \eta_0 \pmod 3$$

$$\eta_1^3 = \alpha^6 + \alpha^5 + \alpha^2 + 3(\alpha^{10} + \alpha^9 + \alpha + \alpha^{12} + \alpha^4 + \alpha^3) + 6 = \eta_1 + 3(\eta_0 + \eta_2) + 6$$

$$\equiv \eta_1 \pmod 3$$

$$\eta_2^3 = \alpha^{12} + \alpha^{10} + \alpha^4 + 3(\alpha^7 + \alpha^5 + \alpha^2 + \alpha^{11} + \alpha^8 + \alpha^6) + 6 = \eta_2 + 3(\eta_1 + \eta_3) + 6$$

$$\equiv \eta_2 \pmod 3$$

$$\eta_3^3 = \alpha^{11} + \alpha^7 + \alpha^8 + 3(\alpha + \alpha^{10} + \alpha^4 + \alpha^9 + \alpha^3 + \alpha^{12}) + 6 = \eta_3 + 3(\eta_0 + \eta_2) + 6$$

$$\equiv \eta_3 \pmod 3$$

**Page 114, Problem 4**. Show that for a prime $\lambda$, any prime factor of $k^{\lambda-1} + k^{\lambda-2} + \cdots + 1$ are either 0 or 1 $\pmod \lambda$. The main thing here is that "any prime factor of" not just that the whole sum is $0, 1 \pmod \lambda$ even though it is.

If $k = 1$ then the sum is exactly $\lambda$ and we have $0 \pmod \lambda$, if $k \neq 1$ then from geometric series we have the sum to be $\frac{k^\lambda - 1}{k - 1} \equiv \frac{k - 1}{k - 1} \equiv 1 \pmod \lambda$ (where we have used Fermat's Little Theorem $k^\lambda \equiv k \pmod \lambda$).

But the above geometric formula also applies mod any prime factor $p$ of the sum (as long as $k \neq 1$), *i.e.* $k^{\lambda-1} + k^{\lambda-2} + \cdots + 1 = \frac{k^\lambda - 1}{k - 1} \equiv 0 \pmod p$, it is $0 \pmod p$ because $p$ is a prime factor of the sum.

This means that $k^\lambda \equiv 1 \pmod p$, therefore it's either $k = 1$ (the only element with order one is $k = 1$) or the order of $k$ mod $p$ is $\lambda$ (because $\lambda$ is prime otherwise the order can be any factor of $\lambda$). But $k = 1$ is already covered above and we have explictly 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 $\lambda$. Then Fermat's Little Theorem tells us that $\lambda | p - 1$ and we immediately have $p \equiv 1 \pmod \lambda$.

**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 $\eta_i \equiv u_i \pmod p$ obeys $u^2 + u - 1 \equiv 0 \pmod p$.

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 $\alpha$) and

$(-1)^2 - 1 - 1 \not\equiv 0 \pmod{19}$. 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 $\eta$.

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 $\eta_i \equiv u_i \pmod{p}$ therefore $u_i^2 + u_i - 1 \equiv 0 \pmod{19}$, solving it we get $u_i(u_i + 1) \equiv 1 \pmod{19}$. The solution is $u_i = 4$ and $u_i = -5$ and these are the only two solutions since we only have two $\eta$.

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 :)

$$Nf(\alpha) = 19 \cdot 19 = \{f(\alpha)f(\alpha^2)\} \cdot \{f(\alpha^3)f(\alpha^3)\}$$
$$= \{19\} \cdot \{19\}$$

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

$$h(\alpha)g(\alpha) = \eta_0 - 4$$
$$Nh(\alpha)Ng(\alpha) = 19^2$$

which means that $Nh(\alpha) = Ng(\alpha) = 19$ for $\eta_0$ to be reducible but just like the proof on Page 113, $Nh(\alpha) = h(1)^{\lambda-1} \equiv 0, 1 \pmod{\alpha - 1}$. From Page 93 we know that $\alpha - 1$ is prime, its norm is $\lambda$ therefore $Nh(\alpha) = h(1)^{\lambda-1} \equiv 0, 1 \pmod{\lambda}$.

In this case $Nh(\alpha) = 19$ so it can't be $0 \pmod{\lambda}$. Thereofore it must be $1 \pmod{\lambda = 5}$ but 19 is not 1 (mod 19) thus contrary to our asuumption, $\eta_0 - 4$ 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)

$$\eta_0 = \alpha + \alpha^4 + \alpha^3 + \alpha^{12} + \alpha^9 + \alpha^{10}$$
$$\eta_1 = \alpha^2 + \alpha^8 + \alpha^6 + \alpha^{11} + \alpha^5 + \alpha^7$$

the multiplication table is

$$\eta_0^2 = \eta_1 + 2(\eta_1 + \eta_0 + 3)$$
$$= 3 - \eta_0$$

this means that if $\eta_0 \equiv u \pmod{p}$ then $u^2 + u - 3 \equiv u(u+1) \equiv 0 \pmod{3}$ 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 $\lambda$ 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, $Nf(\alpha) \equiv f(1)^{\lambda-1} \equiv 0, 1 \pmod{\alpha - 1} \equiv 0, 1 \pmod{\lambda}$

since from Page 93 we know that $\alpha - 1$ is prime and its norm is $\lambda$ (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 assumtion that $0 < a < f$. Therefore, $g(\alpha)$ is irreducible.