Harold Edwards Fermat's last theorem

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: January 10, 2018)

Abstract

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

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

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

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

using the quadratic formula

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Now there might be some other numbers such that

$$DM + ZN = g$$

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

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

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

$$DM' + ZN' = 1$$

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

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

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

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

Now, equating the two Bezouts again

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

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

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

Now, equating the two Bezouts again

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

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

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

and we are done.

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

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

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

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

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

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

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

with both r and s odd and co-prime and

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

with u and v integers and co-prime and so

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

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

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

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

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

since u and v are coprime. Thus

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

and

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

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

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

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

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

What we have is (from the pythagorean triple formula)

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

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

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

Thus, just like above

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

and therefore

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

Thus we have our infinite descent all over again.

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

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

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

Since x^2+3y^2 is odd then one of them is odd and the other even. If y is even then x must be odd, let's list the possibilities. This also means that $3y^2\equiv 0 \pmod 6$, 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 $1 \pmod 6$. Let's check the other possibility, x is even, y odd. An even number (mod 6) can only be of the form $2, 4 \pmod 6$ therefore $x^2 \equiv 4 \pmod 6$, y can only be $1, 5 \pmod 6$, so $y^2 \equiv 1 \pmod 6$, therefore $x^2 + 3y^2 \equiv 1 \pmod 6$.

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 $x \equiv 1, 3, 5, 7 \pmod 8$ and $x^2 \equiv 1 \pmod 8$. On the other hand y can be anything, listing all the squares mod 8 we get $2y^2 \equiv 0, 2 \pmod 8$, thus $x^2 + 2y^2 \equiv 1, 3 \pmod 8$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

as required :)

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

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

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

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

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

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

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

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

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

        # min_s is to hold the current possible minimum of s
        # has to be reset 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)
```

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

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

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

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

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

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

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

line += 1

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

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

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

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

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

            # make sure the outer loop stop
            K = new_K

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


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

with the output

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

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

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

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

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

We need to show that

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

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

First thing we need is

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

therefore the Pell's equation we had earlier becomes

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

we now do the oldest trick in the book, substitutions

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

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

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

and

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

making the substitution

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

multiplying both of them

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The somewhat problematic terms here are the crossed ones

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

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

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

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

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

if n is odd we have

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

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

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

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

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

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

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

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

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

then it *must* also be a solution :)

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

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

Basic and Extra Ingredients

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

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

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

Sinister problems :)

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

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

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

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

Since $t = c - d$