Harold Edwards Fermat's last theorem

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: December 2, 2017)

Abstract

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

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

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

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

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

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

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

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

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

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

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 25, Problem 1. Prove that $2^{37}-1$ is not prime

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

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

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 , 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

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

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

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

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 $B = \pm 1$

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 $F = u-v$

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

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 $Y = I = 1 \to v = 1$ and $Z = v = 0$ and $X = u = 1$, this means $C = u+v = 1$ and $F = u-v = 1$ and $2E^4 = C^4 - F^4 = 1-1 = 0 \to E = 0$, which means one of n or $n+2$ is zero, which also means $8A^4 = n(n+2) = 0 \to A = 0$ 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.

Pell's Equation Permutation.

Right triangles with legs differing by one,

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

$x_{n+2} = 6x_{n+1} - x_n$

$b^2 - 2d^2 = 1$, if $d = 2h^2$ then there's no non-trivial solution.

Since $t = c - d$