Harold Edwards Fermat's last theorem

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: November 28, 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

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

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

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

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

$$1^2 - A0^2 = 1$$

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

$$3^2 - A1^2 = -4$$

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

$$4^2 - A1^2 = 3$$

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

$$7^2 - A2^2 = -3$$

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

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

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

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

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

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