Computer Science Tripos 2018 Paper 2 Question 9
A Discussion Answer

Thomas Forster

April 26, 2021

(a)

I **HATE** Fiddlibonacci questions, but they can be quite useful disciplines. For various reasons. One of them is that you always have to do an induction, and the other is that, once you get into the induction you have to make sure you commit no errors of transcription which in turn means you have to do things slowly and carefully and not rush things, and don't panic, he says, his voice rising...

No, really!

This particular fiddlibonacci question is actually rather good. You are invited to prove:

$$(\forall abn)(\texttt{GCD}(a \cdot F_{n+3} + b \cdot F_{n+2},\quad a \cdot F_{n+1} + b \cdot F_n) = \texttt{GCD}(a, b))$$

You are obviously going to prove this by induction, and by induction on 'n' at that. (I hope you were not expecting to do it by induction on a or b!), However, one needs to take some thought. Do you fix a and b, and then prove, by induction on n—holding a and b constant—that

$$\texttt{GCD}(a \cdot F_{n+3} + b \cdot F_{n+2},\quad a \cdot F_{n+1} + b \cdot F_n) = \texttt{GCD}(a, b)?$$

Or do you prove by induction on n that

$$(\forall ab)(\texttt{GCD}(a \cdot F_{n+3} + b \cdot F_{n+2},\quad a \cdot F_{n+1} + b \cdot F_n) = \texttt{GCD}(a, b))? \qquad (S)$$

...so that you—as it were—carry all the as and b around with you, inside the induction. If you think about it, this second induction is much stronger, beco's you are proving the induction for *all* a and b, not just a single pair. (Your induction hypothesis has a universal quantifier at the front!) I'm keeping fingers crossed that it's the first kind of induction we do.

So fix a and b and consider the case $n = 0$. This requires us to check that

$$\texttt{GCD}(a \cdot F_3 + b \cdot F_2,\quad a \cdot F_1 + b \cdot F_0) = \texttt{GCD}(a, b).$$

Recall that $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$. Evidently $\texttt{GCD}(2a+b, a) = \texttt{GCD}(a, b)$ by the usual manipulations.

Now for the induction step. Let's assume that it holds for n, so that

$$\texttt{GCD}(a \cdot F_{n+3} + b \cdot F_{n+2}, \quad a \cdot F_{n+1} + b \cdot F_n) = \texttt{GCD}(a, b)$$

and we wish to infer

$$\texttt{GCD}(a \cdot F_{n+4} + b \cdot F_{n+3}, \quad a \cdot F_{n+2} + b \cdot F_{n+1}) = \texttt{GCD}(a, b)$$

The obvious thing to reach for is stuff like $\texttt{GCD}(u, v) = \texttt{GCD}(u - v, v)$ so we subtract the second component of the LHS from the first to get the equivalent

$$\texttt{GCD}(a \cdot F_{n+3} + b \cdot F_{n+2}, \quad a \cdot F_{n+2} + b \cdot F_{n+1})$$

... at which point we get stuck. Indeed that was the point at which i ran up the white flag and looked up the model answer kept in the vault by the examiners. It's not very nice. So i decided to go back and attempt instead to prove the much stronger induction (S) above.

First we check the case $n = 0$, as we did earlier. This time we have a '$\forall ab$' to worry about:

$$(\forall ab)(\texttt{GCD}(a \cdot F_3 + b \cdot F_2, \quad a \cdot F_1 + b \cdot F_0) = \texttt{GCD}(a, b))$$

but that causes no extra complication.

So let's try the induction step: suppose

$$(\forall ab)(\texttt{GCD}(a \cdot F_{n+3} + b \cdot F_{n+2}, \quad a \cdot F_{n+1} + b \cdot F_n) = \texttt{GCD}(a, b))$$

holds for n. We want to show that it holds for $n + 1$.

Well,

$$\texttt{GCD}(a \cdot F_{n+3} + b \cdot F_{n+2}, \quad a \cdot F_{n+1} + b \cdot F_n) = \texttt{GCD}(a, b)$$

holds for all a and b, so let's substitute $a + b$ for a, getting

$$\texttt{GCD}((a + b) \cdot F_{n+3} + b \cdot F_{n+2}, \quad (a + b) \cdot F_{n+1} + b \cdot F_n) = \texttt{GCD}(a, b)$$

(This thing, for our given value of 'n', holds for all a and b.)

We can rearrange $(a + b) \cdot F_{n+3} + b \cdot F_{n+2}$ into $a \cdot F_{n+3} + b \cdot (F_{n+3} + F_{n+2})$ which is of course $a \cdot F_{n+3} + b \cdot F_{n+4}$. And we can rearrange $(a+b) \cdot F_{n+1} + b \cdot F_n$ analogously into $a \cdot F_{n+1} + b \cdot F_{n+2}$.

This means we have proved

$$\texttt{GCD}(b \cdot F_{n+4} + a \cdot F_{n+3}, \quad b \cdot F_{n+2} + a \cdot F_{n+1}) = \texttt{GCD}(a + b, b)$$

But of course $\texttt{GCD}(a + b, b) = \texttt{GCD}(a, b)$ so we get

$$\texttt{GCD}(b \cdot F_{n+4} + a \cdot F_{n+3}, \quad b \cdot F_{n+2} + a \cdot F_{n+1}) = \texttt{GCD}(a, b)$$

and this holds for all a and b.

In effect we have swapped the variables 'a' and 'b' around and incremented n. But the induction hypothesis was that it held for all a and b so we're happy.

Mind you, Gareth Taylor seems to have found a nice way of getting the first proof to work. (Nicer than the embargoed answer in the examiners' vault.) He says:

> Am I being sleepy (I am yawning a lot), or is the induction okay?
>
> Let's assume $\texttt{GCD}(a \cdot F_{n+3} + b \cdot F_{n+2},\ a \cdot F_{n+1} + b \cdot F_n) = \texttt{GCD}(a, b)$
>
> Via $\texttt{GCD}(u, v) = \texttt{GCD}(u - v, v)$ we get
>
> $\texttt{GCD}(a \cdot F_{n+2} + b \cdot F_{n+1},\ a \cdot F_{n+1} + b \cdot F_n) = \texttt{GCD}(a, b)$
>
> Via $\texttt{GCD}(u, v) = \texttt{GCD}(u, u + v)$ we get
>
> $\texttt{GCD}(a \cdot F_{n+2} + b \cdot F_{n+1},\ a \cdot F_{n+3} + b \cdot F_{n+2}) = \texttt{GCD}(a, b)$
>
> Via $\texttt{GCD}(u, v) = \texttt{GCD}(u, u + v)$ again we get
>
> $\texttt{GCD}(a \cdot F_{n+2} + b \cdot F_{n+1},\ a \cdot F_{n+4} + b \cdot F_{n+3}) = \texttt{GCD}(a, b)$

(b)

Observe that $\bigcup \mathcal{F}$ is one of the things that $\supseteq$ everything in $\mathcal{F}$, so certainly $\bigcup \mathcal{F} \in \mathcal{G}$, whence $\bigcap \mathcal{G} \subseteq \bigcup \mathcal{F}$. For the other direction we want $\bigcup \mathcal{F}$ to be included in every member of $\mathcal{G}$. But every g in $\mathcal{G}$ extends every member of $\mathcal{F}$, so certainly g extends $\bigcup \mathcal{F}$ as desired.

The best way to visualise this is to think of the power set of T as a Hasse diagram, so that $\mathcal{F}$ and $\mathcal{G}$ as *regions* of the Hasse diagram. $\mathcal{G}$ is the collection of those nodes in the Hasse diagram that are above everything in $\mathcal{F}$.

(c)

I'll get round to this if you push me hard enough.