Computer Science Tripos 2018 Paper 2 Question 7
A Discussion Answer

Thomas Forster

May 29, 2023

I'm not going to do part (a). I'm a logician, not some sad number theorist.

Oh, all right, just so you don't think i can't do it. $(x+3)(x+2) = 0$ mod 187. So we are looking for xs that are congruent to -3 or -2 mod 187. Now $187 = 11 \cdot 17$, so we are looking for xs that are congruent to -3 or -2 mod 11 or 17. Or, to put it another way, we are looking for x s.t. $(x+3)(x+2)$ is divisible both by 11 and by 17. So we are looking for a multiple of 11 and a multiple of 17 (both less than 187) that differ by 1. (Beco's $x+3$ and $x+2$ differ by 1) 34 and 33 are looking good, so $x = 31$ works; and there's 184 and 185 as well, giving 182; and 153 and 154, giving $x = 151$. That's yer lot.

(b)

This is pretty trivial stuff really, so the only work involved comes from the need to understand the notation and to manipulate it properly. That can be a pain. However this question serves to make one point: (thank you Miss Kuchma of Queens'!) If (b)(ii) is to be true then $\mathbb{N}$ had better have 0 as a member. (Sad number theorists think that $0 \notin \mathbb{N}$—i mean *really* ...). Suppose 0 is not a natural number. Think about what happens to (b)(ii) if you take $m = 1$ and $l = 2$; ($l > 1$ is enuff). Then the LHS is empty and the RHS is not.

(i) Resist the temptation to send $\langle x, y\rangle$ to $x \cdot y$. (Why?[1])

(ii) Easy-peasy lemon-squeezy.

(iii) I think this is quite tricky to get right, and offering only 8 marks for a correct answer looks a bit stingey to me. I would give at least a Queens' mini-mint.

The first thought i had was that, since $\oplus$ is defined by recursion on the *second* argument, one would have to prove the target proposition by induction on the second argument. But then the thing you're trying to prove is symmetrical in the two arguments, so perhaps the proof has to be symmetrical too.

Then one notices that

$$|[m] \oplus [n+1]| = |[m] \oplus [n]| + 1 \qquad (***)$$

[1] It's not injective!

and that one can prove this directly, for all m and n, by UG not by induction. (Don't overlook the vertical bars—signifying cardinality—in that last formula, in the forest of verticals, with [and] and |s. . . .)

Then one notices that one is *not* being asked to prove that $|[m] \oplus [n]| = m + n$—even though that looks obvious, and is presumably true. That would be hard work.

So i think it works like this. You use (***) to show, by induction on n, that

$$|[m] \oplus [n]| = |[m] \oplus [0]| + n$$

But $|[m] \oplus [0]| = m$ whence

$$|[m] \oplus [n]| = m + n.$$

But of course we also get

$$|[n] \oplus [m]| = n + m$$

whence

$$|[m] \oplus [n]| = |[n] \oplus [m]|$$

as desired.

That's a short and quick proof, but it took your humble correspondent several attempts to get it. Definitely an example sheet question rather than an exam question.

I have just realised why i have this feeling of *déja vu* about this question. That is because i wrote a discussion answer to an earlier incarnation of this question in
`https://www.dpmms.cam.ac.uk/~tf/cam_only/2013p2q5.pdf`
and readers should visit *that*.