Hi Francesca,

I’ve managed to fill in the rest on my way home on the train. Here’s my argument.

I am looking for $aX+b$ in $Z_{44}[X]$ such that $(aX+b)(22X+25)=1$ in $Z_{44}[X]$.

Expanding the LHS, this amounts to finding integers a and b in $Z_{44}$ such that

$22a\equiv 0$ (the coefficient of $X^2$)

$25a+22b\equiv 0$ (the coefficient of X)

$25b\equiv 1$  (the constant term)

in $Z_{44}$.

Let’s start with b. To find b, we need to find a pair of integers b and d such that $25b+44d=\gcd(25, 44)=1$. Granted, $25b\equiv 1 \bmod 44$. One can make appeal to Euclid’s algorithm or otherwise to see $25*(-7)+44*4=1$, so $b\equiv (-7) \bmod 44$ does the job.

For a, one may observe that it needs to be an even integer (because 22a has to be divisible by 44), i.e., $a=2c$ for some integer c.

Combing these two, our task is then to find c such that the coefficient of X:$25a+22b=50c+22*(-7)\equiv 0 \bmod 44$, i.e., solve $50c\equiv 154 \bmod 44$.

How do we find c? Our intermediate goal is to find a pair of integers d and e such that $50d+44e=\gcd(55, 44)=2$. Once we find a such pair, then $50*(77d)+44*(77d)=2*77=154$, so we get $c=77d$.

How do we find d and e then? Well, we run Euclid’s algorithm again with 50 and 44! If you do this exercise, we find $50*(-7)+44*8=\gcd(50, 44)=2$, i.e. $(d, e)=(-7, 8)$. So feeding this back into the argument above, $c=(-7)*77=(-539)\equiv 33 \bmod 44$.

Of course what we want is a and this is given by $a=2c\equiv 2*33=66\equiv 22 \bmod 44$. On the other hand $b=(-7)\equiv 37 \bmod 44$. So the answer you are looking for is $[22]X+[37]$ in $Z_{44}[X]$.

Looking back, a=22 seems like an `obvious thing’ to do!