KMB, 26/11/18

M1F Foundations of Analysis, Problem Sheet 8, solutions.

1. Say (x, y) is a solution. The left hand side is a square and hence non-negative, so $x \geq -1$. If $x = -1$ then $y = 0$ is the only thing that works, if $x = 0$ then nothing works, so we may assume $x \geq 1$, and our job is to prove that this can't happen. Under this assumption we can't have $y = 0$, so by changing the sign of y if necessary we can assume $y \geq 1$. Now $(6y-1)$ and $(6y+1)$ are both positive integers whose product is a fifth power, and they are coprime because they are clearly both odd and any common divisor divides their difference, which is two. Hence they are both fifth powers, by Proposition 7.15. However no positive two 5th powers can differ by two – indeed even consecutive positive 5th powers always differ by more.

2. (i) As in the hint we write $N = N(\lambda a + \mu b) = \lambda Na + \mu Nb$. Now N is a multiple of a, so Nb is a multiple of ab, and N is a multiple of b so Na is a multiple of ab as well. Hence $\lambda Na + \mu Nb$ is the sum of some multiples of ab, so N is a multiple of ab.

(ii) Applying (i) we see that if $x - y$ is a multiple of p and of q then it's a multiple of pq. Now applying it again with $a = pq$ and $b = r$ (which are coprime because r does not divide pq and r is prime) we see that $x - y$ is a multiple of pqr and hence x is congruent to y modulo pqr. The converse is easy.

(iii) We have $2^7 - 2 = 126 = 2 \times 9 \times 7$. However 9 clearly does not divide $3^7 - 3$, because it does divide 3^7 and it doesn't divide 3. Hence the highest common factor of $2^7 - 2$ and $3^7 - 3$ must divide $2 \times 3 \times 7 = 42$.

But now I claim that 42 is the answer. To check this all we need to do is to check that $n^7 - n$ is a multiple of 42 for $2 \leq n \leq 1000$ and to check this it would suffice to show that $n^7 - n$ is a multiple of 42 for all integers n. To do this, by the previous part, it suffices to show that $n^7 - n$ is always a multiple of 2, of 3 and of 7. Let's deal with these cases separately.

We see $n^7 - n$ is always a multiple of 2 by checking the two cases. Either n is odd, in which case n^7 is odd so the difference is even, or n is even in which case n^7 is even, so the difference is even. In either case the difference is even.

We next want to prove that $n^7 - n$ is always a multiple of 3. One trick way to do this would be to notice that $n^7 - n = n(n^6 - 1) = n(n^2 - 1)(1 + n^2 + n^4) = (n^3 - n)(1 + n^2 + n^4)$ and that $n^3 - n$ is always a multiple of 3 by Fermat's Little Theorem; one could also check the three cases $n \equiv 0, 1, 2 \bmod 3$ separately.

Finally we want to prove that $n^7 - n$ is always a multiple of 7, but this follows immediately from Fermat's Little Theorem once we have checked that 7 is prime, which it is, because it's not a multiple of 2,3,4,5 or 6.

So we're done!

(iv) By part (ii) it suffices to check that $n^{561} - n$ is always a multiple of 3, of 11 and of 17. We do this by generalising Fermat's Little Theorem thus:

Theorem. If p is prime, and if e is a positive integer congruent to 1 mod $p - 1$, then for every integer n we have that $n^e - n$ is a multiple of p.

Proof. If n is a multiple of p this is clear. If not then by Fermat's Little Theorem we have $n^{p-1} \equiv 1 \bmod p$. Now write $e = d(p-1) + 1$, and observe that $n^{e-1} = (n^{p-1})^d \equiv 1^d \equiv 1 \bmod p$, and hence $n^e \equiv n \times 1 \equiv n \bmod p$.

We can now deduce (iv) because it's easy to check that 560 is a multiple of 2, 10 and 16.

3.

(i) We have $a \leq a$ for all a so $\sim$ is reflexive. We have $1 \leq 2$ but $2 \not\leq 1$, so $\sim$ is not symmetric. If $a \leq b$ and $b \leq c$ then $a \leq c$, so $\sim$ is transitive.

(ii) $a - a = 0 = 0^2$, so $\sim$ is reflexive. We have $2 \sim 1$ as $2 - 1 = 1^2$, but $1 \not\sim 2$ as -1 is not a square, so the relation is not symmetric. Finally we have $3 \sim 2$ and $2 \sim 1$ but $3 \not\sim 1$ as 2 is not a square, so $\sim$ is not transitive either.

(iii) $2 \neq 2^2$ so $2 \not\sim 2$, and $\sim$ is not reflexive. We have $4 \sim 2$ but $2 \not\sim 4$ as $2 \neq 4^2$, so the relationship is not symmetric. We have $4 \sim 2$ and $16 \sim 4$ but $16 \not\sim 2$ so the relation is not transitive.

(iv) We have $1 \not\sim 1$ so $\sim$ is not reflexive. If $a \sim b$ then $a + b = 0$, so $b + a = 0$, so $b \sim a$, hence $\sim$ is symmetric. Finally we have $1 \sim -1$ and $-1 \sim 1$ but $1 \not\sim 1$ so $\sim$ is not transitive.

(v) We have $a - a = 0$ is an integer, so $\sim$ is reflexive. If $a - b$ is an integer then so is $b - a$, so $\sim$ is symmetric. Finally if $a - b$ and $b - c$ are integers, then their sum is $a - c$ which is also an integer. So $a \sim b$ and $b \sim c$ implies $a \sim c$, and in particular $\sim$ is also transitive. So in fact this relation is an equivalence relation.

(vi) $2 \not\sim 2$ so $\sim$ is not reflexive. We know $1 \sim 3$ but $3 \not\sim 1$ so $\sim$ is not symmetric. It is however impossible to find $a, b, c \in S$ with $a \sim b$ and $b \sim c$ (because b would have to be 1 and 3) so the statement "$a \sim b$ and $b \sim c$ implies $a \sim c$" is true, as if P is false then "P implies Q" is always true whatever the truth value of Q. So this relation is transitive.

(vii) This relation is reflexive, symmetric and transitive, because it is impossible to find any counterexamples to these statements as S is empty (for example for $\sim$ not to be reflexive we would have to find $a \in S$ with $a \not\sim a$, but we can't find any $a \in S$ at all, so $\sim$ is reflexive etc etc).

4.

(i) If $\sim$ is reflexive then $0 \sim 0$ and hence $0 = 0 - 0 \in X$.

Conversely if $0 \in X$, then for all $a \in \mathbf{R}$ we have $a - a = 0 \in X$, so $a \sim a$. But $a \in \mathbf{R}$ was arbitrary, so $\sim$ is reflexive.

(ii) For $\implies$: Say $\sim$ is symmetric, and choose $x \in X$. We need to show that $-x \in X$. But $x - 0 = x \in X$, so $0 \sim x$. By symmetry, $x \sim 0$, and by definition of $\sim$ we have $0 - x = -x \in X$.

Conversely, say $x \in X \implies -x \in X$, and let's choose $a, b \in \mathbf{R}$ with $a \sim b$. We want to prove $b \sim a$. But $x := b - a \in X$ by definition of $a \sim b$. So $-x \in X$, so $a - b \in X$, so $b \sim a$. Because a, b were arbitrary, we deduce that $\sim$ is symmetric.

(iii) For the $\implies$ direction: assume $\sim$ is transitive, and choose $x, y \in X$. Then $0 \sim x$ and $x \sim x + y$, so by transitivity we have $0 \sim x + y$, and hence $x + y \in X$.

Conversely, say $a, b, c \in \mathbf{R}$ and $a \sim b$ and $b \sim c$. Then $x := b - a \in X$ and $y := c - b \in X$, hence $x + y \in X$ by assumption. But $x + y = c - a$, so $a \sim c$. As a, b, c were arbitrary, we deduce that $\sim$ is transitive.

5.

(i) To prove that it *is* possible to show that reflexive and transitive implies symmetric, we just have to write down a proof that if $\sim$ is any binary relation on any set S and $\sim$ is reflexive and transitive, then $\sim$ is symmetric. To prove that it is *not* possible, we need to write down a counterexample, which in this context would mean an example of a set S and a binary relation $\sim$ which is reflexive and is transitive but is not symmetric.

(ii) We know $a \leq a$ for all a, so $\sim$ is reflexive. We also know that $a \leq b$ and $b \leq c$ implies $a \leq c$, so $\sim$ is transitive. But $\sim$ is not symmetric because $3 \sim 4$ but $4 \not\sim 3$.

(iii) If $x \in \mathbf{R}$ then $|x - x| = 0 \leq 1$, so $x \sim x$. Hence $\sim$ is reflexive. Next, if $|x - y| \leq 1$ then $|y - x| = |-(x - y)| = |x - y| \leq 1$, so $\sim$ is symmetric. However $1 \sim 2$ and $2 \sim 3$ but $1 \not\sim 3$, so $\sim$ is not transitive.

(iv) $0 \sim 0$ is false, so $\sim$ is not reflexive. However $\sim$ is symmetric and transitive, because whatever x and y are, $(x \sim y)$ is always false, so $(x \sim y) \implies (y \sim x)$ is true (because false implies anything). Similarly transitivity is true (because false implies anything).

6. The mistake is that you might not be able to choose t with $s \sim t$, because perhaps there are no $t \in S$ at all (including $t = s$) satisfying $s \sim t$.