KMB, 30/11/17

M1F Foundations of Analysis, Problem Sheet 8, solutions.

1. We know from lectures that there exists integers λ and μ such that $\lambda a + \mu b = 1$. If m is some positive integer then we can deduce that $\lambda ma + \mu mb = m$. So it looks like we can just buy λm boxes of a nuggets and μm boxes of b nuggets and we will be done – until we notice that λ and μ are unlikely to both be non-negative, so probably either λm or μm will be less than zero.

So what do we do? Well, in the last sheet we saw a trick: if we have a solution to $Xa+Yb = m$ with X and Y integers, then we can subtract b from X, getting $X' = X-b$, and add a to Y getting $Y' = Y+a$, and then $X'a+Y'b$ is also m, because $X'a+Y'b = Xa-ba+Yb+ab = Xa+Yb = m$. More generally if $X' = X - qb$ and $Y' = Y + qa$ for any integer q, then $X'a + Y'b = m$ (easy check).

Now I claim that we can set $N = ab$. Here's why. The argument above shows that for any integer $m \geq N$ (and indeed any integer m at all) we can solve $Xa+Yb = m$ in *integers* X and Y, not yet worrying about whether they are positive or not. Now let's use the trick of changing X by a multiple of b and Y by a multiple of a. More precisely, let's try and change X so that it's as small as possible but still at least zero. So let's write $X = qb + r$ (quotient and remainder) with $0 \leq r < b$, and let's set $X' = X - qb$ and $Y' = Y + qa$. We've just seen that $X'a + Y'b = m$. But furthermore in this case we have $X' = qb + r - qb = r$, so $0 \leq X' < b$. In particular X' is non-negative and at most b. But now $Y' = (m - X'a)/b \geq (m - ba)/b \geq 0$ (because we assumed $m \geq ab$), so Y' is also non-negative, and this is what we wanted.

Note that actually figuring out the *smallest* N such that we can always buy m nuggets if $m \geq N$, is harder. We know $N \leq ab$ from this question, but if you are more careful you can figure out what the smallest N is exactly (hint: it's closer to $(a - 1)(b - 1)$ in general).

I'll finish by noting that if we can instead by either a, b or c nuggets, then finding an explicit formula for the largest number you can't buy is an open problem, although of course for any given explicit set of integers one can solve it. For a general finite set of possible nugget purchases, the problem of finding the largest number you can't buy is actually NP hard. Google for "Frobenius coin problem" or "Frobenius stamp problem" for more information about this question.

2*. (i) is true. For if a positive integer d divides a and b then it must divide $\lambda a + \mu b$ and hence it divides 1, so it is at most 1. In particular the only positive integer common factor of a and b is 1, so a and b are indeed coprime.

(ii) is false. For example if $a = b = 1$ then we can set $\lambda = 3$ and $\mu = 4$.

3. (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.

4.

(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).

5.

(i) If $a \in \mathbf{R}$ then $a - a = 0 \in G$, so $a \sim a$. But $a \in \mathbf{R}$ was arbitrary, so $\sim$ is reflexive.

(ii) Say $a, b \in \mathbf{R}$ and $a \sim b$. Then $g := b - a \in G$ by definition. So $-g \in G$, so $a - b \in G$, so $b \sim a$. But a, b were arbitrary, so $\sim$ is symmetric. (iii) Say $a, b, c \in \mathbf{R}$ and $a \sim b$ and $b \sim c$. Then $g := b - a \in G$ and $h := c - b \in G$, hence $g + h \in G$. But $g + h = c - a$, so $a \sim c$. But a, b, c were arbitrary, so $\sim$ is transitive.

(iv) If $\sim$ is reflexive then $0 \sim 0$ so $0 - 0 \in G$ hence $0 \in G$. If $\sim$ is symmetric then for $g \in G$ we have $0 \sim g$, so $g \sim 0$, so $-g \in G$. Finally if $\sim$ is transitive then for $g, h \in G$ we have $0 \sim g$ and $g \sim g + h$, so $0 \sim g + h$ hence $g + h \in G$.