KMB, 30/11/17

## M1F Foundations of Analysis, Problem Sheet 8.

**1.** Let $a$ and $b$ be coprime positive integers (recall that *coprime* here means $\gcd(a,b)=1$). I open a fast food restaurant which sells chicken nuggets in two sizes – you can either buy a box with $a$ nuggets in, or a box with $b$ nuggets in. Prove that there is some integer $N$ with the property that for all integers $m \geq N$, it is possible to buy exactly $m$ nuggets.

**2*.** True or false?

(i) If $a$ and $b$ are positive integers, and there exist integers $\lambda$ and $\mu$ such that $\lambda a+\mu b=1$, then $\gcd(a,b)=1$.

(ii) If $a$ and $b$ are positive integers, and there exist integers $\lambda$ and $\mu$ such that $\lambda a+\mu b=7$, then $\gcd(a,b)=7$.

**3.** (i) Say $a$ and $b$ are coprime positive integers, and $N$ is any integer which is a multiple of $a$ and of $b$. Prove that $N$ is a multiple of $ab$. Hint: we know that $\lambda a+\mu b=1$ for some $\lambda,\mu\in\mathbf{Z}$; now write $N=N\times(\lambda a+\mu b)$.

(ii) By applying (i) twice, deduce that if $p$, $q$ and $r$ are three distinct primes, then two integers $x$ and $y$ are congruent modulo $pqr$ if and only if they are congruent mod $p$, mod $q$ and mod $r$.

(iii) (tough) Consider the set of positive integers $\{2^7-2, 3^7-3, 4^7-4, \ldots, 1000^7-1000\}$. What is the greatest common divisor of all the elements of this set? Feel free to use a calculator to get the hang of this; feel free to use Fermat's Little Theorem and the previous part to nail it.

(iv) (tougher) $561 = 3\times 11\times 17$. Prove that if $n\in\mathbf{Z}$ then $n^{561}\equiv n \bmod 561$. Hence the converse to Fermat's Little Theorem is false.

**4.** For each of the following binary relations on a set $S$, figure out whether or not the relation is reflexive. Then figure out whether or not it is symmetric. Finally figure out whether or not the relation is transitive.

(i) $S=\mathbf{R}$, $a\sim b$ if and only if $a\leq b$.

(ii) $S=\mathbf{Z}$, $a\sim b$ if and only if $a-b$ is the square of an integer.

(iii) $S=\mathbf{R}$, $a\sim b$ if and only if $a=b^2$.

(iv) $S=\mathbf{Z}$, $a\sim b$ if and only if $a+b=0$.

(v) $S=\mathbf{R}$, $a\sim b$ if and only if $a-b$ is an integer.

(vi) $S=\{1,2,3,4\}$, $a\sim b$ if and only if $a=1$ and $b=3$.

(vii) $S$ is the empty set (and $\sim$ is the only possible binary relation on that set, the empty binary relation).

**5.** Let $S=\mathbf{R}$ be the real numbers, and let $G$ be a subset of $\mathbf{R}$. Define a binary relation $\sim$ on $S$ by $a\sim b$ if and only if $b-a\in G$.

(i) Say $0\in G$. Prove that $\sim$ is reflexive.

(ii) Say $G$ has the property that $g\in G$ implies $-g\in G$. Check that $\sim$ symmetric.

(iii) Say $G$ has the property that if $g\in G$ and $h\in G$ then $g+h\in G$. Check that $\sim$ is transitive.

(iv) If you can be bothered, also check that the converse to all these statements are true as well (i.e. check that if $\sim$ is reflexive then $0\in G$, if $\sim$ is symmetric then $g\in G$ implies $-g\in G$ etc).

Remark: Subsets $G$ of $\mathbf{R}$ with these three properties in parts (i)–(iii) are called *subgroups* of $R$, or, more precisely, additive subgroups (the group law being addition). So this question really proves that the binary relation defined in the question is an equivalence relation if and only if $G$ is a subgroup of $\mathbf{R}$. You'll learn about groups and subgroups next term in M1P2.