M1F Foundations of Analysis — Problem Sheet 4

1. Suppose that a and $b \neq 0$ are integers. Prove that there exist integers q, r (the "quotient" and "remainder") such that $a = qb + r$ where $|r| \leq |b|/2$.

   Using this to allow negative remainders in Euclid's algorithm, can you bound how many steps you need to do to find $\text{hcf}(a, b)$?

   Wlog can take a, b positive. In lectures we showed we could do this with $0 \leq r < b$. If $r \leq b/2$ we're done. If $r > b/2$ then replace q by $q + 1$ and therefore r by $r - b$. Then since $b/2 < r < b$ we find that $-b/2 < (r - b) < 0$ so we've got remainder whose absolute value is $< b/2$.

   Or: could do it from first principles as in lectures by letting

   $$S = \{x \in \mathbb{Z}: a - xb \geq -b/2\}$$

   and showing that S is nonempty and bounded above and letting $q = \max S$. Then proceed as before.

   Thus, in Euclid's algorithm, we divide the smallest of the two numbers by at least 2 at each stage. Therefore after $\sim \log_2 b$ steps, the smallest number is down to 0 and we've finished.

2. For each relation $\sim$ below, state which of symmetric, reflexive, transitive and an equivalence relation it is. ($\lfloor x \rfloor$ denotes the integer part of x, i.e. the largest integer $n \leq x$.)

   (a) On $\mathbb{R}$, $x \sim y \iff \lfloor x \rfloor = \lfloor y \rfloor$.

   (b) On $\mathbb{R}$, $x \sim y \iff \exists n \in \mathbb{Z}$ such that $x, y \in [n - 0.5, n + 0.5)$.

   (c) On $\mathbb{R}$, $x \sim y \iff |x - y| < 1$.

   (d) On $\mathbb{Z}$, $x \sim y \iff |x - y| < 1$.

   (a) Equivalence relation, corresponding to the partition $\coprod_{n \in \mathbb{Z}} [n, n + 1)$ of $\mathbb{R}$.

   (b) Equivalence relation, corresponding to the partition $\coprod_{n \in \mathbb{Z}} [n - 0.5, n + 0.5)$ of $\mathbb{R}$.

   (c) Symmetric, reflexive but not transitive as $0 \sim 0.5 \sim 1$ but $0 \not\sim 1$.

   (d) For $x, y \in \mathbb{Z}$, $|x - y| < 1 \iff x = y$ so this is the equivalence relation $=$ on $\mathbb{Z}$.

3.* (a) How many relations are there on a finite set S ?

   (b) How many reflexive relations ?

   (c) How many symmetric relations ?

   (d) How many symmetric, reflexive relations ?

   (a) Number of subsets of $S \times S$ equals $2^{|S \times S|} = 2^{|S|^2}$.

   (b) Number of subsets of $S \times S$ that contain the diagonal $\Delta_S := \{(s, s): s \in S\}$. Subset defined by a choice, for each element of $(S \times S) \backslash \Delta_S$, of whether it is in the set of not. So we get $2^{|(S \times S) \backslash \Delta_S|} = 2^{|S|^2 - |S|}$ choices, so that many reflexive relations.

   (c) Write $S = \{x_1, \ldots, x_n\}$. Symmetric relation $R \subset S \times S$ is a choice, for each $i \leq j$, of whether or not (x_i, x_j) is in the relation. (We then make the same choice for (x_j, x_i).)
   There are $(n^2 - n)/2 + n = (n^2 + n)/2$ elements $(x_i, x_j) \in S \times S$ with $i \leq j$. Therefore we have $2^{(n^2+n)/2}$ choices and that many symmetric relations.

   (d) Write $S = \{x_1, \ldots, x_n\}$. Symmetric reflexive relation $R \subset S \times S$ is a choice, for each $i < j$, of whether or not (x_i, x_j) is in the relation. (We then make the same choice for (x_j, x_i), while all (x_i, x_i) are always in R.)
   There are $(n^2 - n)/2$ elements $(x_i, x_j) \in S \times S$ with $i < j$. Therefore we have $2^{(n^2-n)/2}$ choices and that many symmetric reflexive relations.

4. Define a relation on the set $\mathbb{Z}$ by $x \sim y$ if and only if $x \equiv y \pmod{n}$.
   Show this is an equivalence relation. What are the equivalence classes ? How many are there ?

   Working mod n, $x \equiv x$ is true for all x, so $\sim$ reflexive. If $x \equiv y$ then $y \equiv x$, so symmetric. If $x \equiv y \equiv z$ then $x \equiv z$, so transitive.

   Equivalence classes are $[i] = \{i + nm: m \in \mathbb{Z}\}$ – the set of integers whose remainder is i when dividing by n. There are n of them, where i runs through $0, 1, 2, \ldots, n - 1$.

5. Find all solutions of the equation $5n + 2 = m^3$ $(m, n \in \mathbb{Z})$.

Working mod 5**, the integer** m **is one of** $0, 1, 2, 3, 4$**, with cubes** $0, 1, 3, 2, 4$ **respectively. So the solutions of** $m^3 \equiv 2$ **(mod 5) are precisely** $m \equiv 3$ **(mod 5).**

So $m = 5k + 3$ **for some** $k \in \mathbb{Z}$**. Thus** $m^3 = 125k^3 + 3.3.25k^2 + 3.3^2.5k + 3^3 = 5(25k^3 + 15k^2 + 27k + 5) + 2$**.**

Therefore $m^3 = 5n + 2$ **iff** $n = 25k^3 + 45k^2 + 27k + 5$**.**

So the solutions are $(m, n) = (5k + 3, 25k^3 + 45k^2 + 27k + 5)$ **for all** $k \in \mathbb{Z}$**.**

6. (Mini RSA.) Let p be a prime, and fix some e coprime to $(p - 1)$.

   (a) Show that there exists d such that $de \equiv 1 \bmod p - 1$.

   (b) Show that we can solve the equation $y \equiv x^e \bmod p$ by $x \equiv y^d \bmod p$.

   Briefly discuss any relevance for coding.

By Euclid there exist d, λ **such that** $de - \lambda(p - 1) = 1$**. Therefore** $de \equiv 1$ **mod** $p - 1$**.**

Working mod p**,** $y^d \equiv x^{ed} \equiv x.x^{\lambda(p-1)}$**.**

By Fermat's little theorem, either $x \equiv 0$ **(in which case** $y = 0$ **and everything is obvious) or** $x^{p-1} \equiv 1$ **so that** $x^{\lambda(p-1)} \equiv 1$ **and the above becomes** $y^d \equiv x$**.**

This could be used for encoding – it encodes numbers x **smaller than** p **as other numbers** y **mod** p**, and is invertible (can be decoded) by setting** $x = y^d$ **mod** p**. But it can't be used like RSA – you can't reveal the key** (p, e) **because if you did then I could work out** d**. So you have to keep the method of encoding secret.**

7. Let p be a prime, and fix a which is *not* equal to 0 or 1 modulo p. Prove that $1 + a + \ldots + a^{p-2} \equiv 0 \bmod p$.

By Fermat's little theorem, $a^{p-1} \equiv 1$ **mod** p**.**

Therefore p **divides** $a^{p-1} - 1 = (a - 1)(1 + a + \ldots a^{p-2})$**.**

But $a \not\equiv 1$ **mod** p**, so** p **does not divide** $a - 1$**. Therefore** p **divides** $1 + a + \ldots a^{p-2}$**.**