Part IA — Numbers and Sets

Supervised by Dr. Forster
Solutions presented by Christopher Turnbull

Michaelmas 2017

1D 2012

(i) By Euclid,

$$\begin{aligned}
23 &= 18 + 5 \\
18 &= 3 \times 5 + 5 \\
5 &= 3 + 2 \\
3 &= 2 + 1
\end{aligned}$$

So gcd(23,18) $= 1$.

Now expressing 1 as a linear combination of 23 and 18,

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) \\
&= 2 \times 3 - 5 \\
&= 2(18 - 5 \times 3) - 5 \\
&= 2 \times 18 - 7 \times 5 \\
&= 2 \times 18 - 7 \times (23 - 18) \\
&= 9 \times 18 - 7 \times 23
\end{aligned}$$

Hence multiplying by 101,

$$909 \times 18 - 707 \times 23 = 101$$

we see that

$$x = 909, y = -707$$

(ii) We know

$$\begin{aligned}
9 \times 18 &= 1 \pmod{23} \\
-7 \times 23 &= 1 \pmod{18}
\end{aligned}$$

So put

$$x = (9 \times 18 \times 2) - (7 \times 23 \times 3)$$

ie.

$$x = 106$$

2D 2012

A relation aRb on elements of a set $a, b \in X$ is an *equivalence relation* if it is

- Reflexive: $aRa \; \forall \; a \in X$
- Symmetric: $aRb \iff bRa \; \forall \; a, b \in X$
- Transitive: aRb and $bRc \Rightarrow aRc \; \forall \; a, b, c \in X$

If $\sim$ is an equivalence relation on X, then the equivalence classes of $\sim$ form a partition of X

Proof. By reflexivity, $x \in [x] \; \forall \; x \in X$.

Now suppose $[x] \cap [y] \neq \emptyset$. Let $z \in [x] \cap [y]$. Then $x \sim z$ and $y \sim z$. By symmetry, $z \sim y$. By transitivity, $x \sim y$.

For all $x' \in X$, we have $x' \sim x$, thus by transitivity, $x' \sim y$, and $[x] \subseteq [y]$. Similarly, $[y] \subseteq [x]$, and $[x] = [y]$. □

(i) V is an equivalence relation: $xRx, xSx \; \forall \; x \in X$ hence $xVx \; \forall \; x \in X$. Similarly, symmetry and transitivity follow exactly.

(ii) W is not necessarily an equivalence relation: take $X = \{1, 2, 3\}$, let R act such that $1R2$, with 3 in its own equivalence class, and let S act such that $2S3$ with 1 in it's own class.

By the definition of W, $1W2$ and $2W3$, but 1 is not related to 3, so transitivity fails.

5D 2012

(i) Not true if X is infinite. Let $X = \mathbb{N}$, $g(x) = x + 1$,

$$f(x) = \begin{cases} 1 & \text{if } x = 1 \\ x - 1 & \text{otherwise} \end{cases}$$

Then $f \circ g$ is the identity map, but $g(f(1)) = 2$.

If X is finite and $f \circ g$ is the identity,

- $f \circ g$ is injective
- $f \circ g$ injective $\Rightarrow g$ injective
- X finite, g injective $\Rightarrow g$ bijective
- $\Rightarrow$ f bijective, $f = g^{-1}$,
- Hence $f \circ g$ identity $\Rightarrow g \circ f$ identity

(ii) Can be false: Let $X \subseteq \mathbb{N}$, take $g(x)$ to be the constant function $g(x) = 1$, and take $f(x) = x^2$.

("g destroys a lot of information, f has a lot of leeway")

(iii) Take $f(x) = 1$ for all $x \in X$. It doesn't matter what g does now, but certainly need not be the identity, for any set X.

- If X is a finite set, for each $x_i \in X$ there exists a positive integer n_i such that $f^{n_i}(x_i) = x_i$. Now simply take $\text{lcm}(x_1, \cdots, x_N)$, thus $f^N(x) = x$ for all $x \in X$
- If X is a countably infinite set, biject it with $\mathbb{N}$ and take the function that maps

$$f(1) = 2, f(2) = 1$$
$$f(3) = 4, f(4) = 5, f(5) = 3$$

and so on. Respectively we have $n = 2, 3, \cdots$, and there is no positive integer N such that $f^N(x) = x$ for all $x \in X$

- If X is an uncountably infinite set, eg. $\mathbb{R}$, simply set the function to be equal to the identity map on the points in $\mathbb{R} \setminus \mathbb{N}$, and equal to our previous function for points in $\mathbb{N}$.

(we can always biject eg. $\mathbb{R}^2 to \mathbb{R}$)

6D 2012

Theorem. Fermat's (Little) Theorem. Let p be a prime. Then $a^p \equiv a$ (mod p), for all $a \in \mathbb{Z}$.

Theorem. Wilsons Theorem. Let p be a prime. Then $(p-1)! \equiv -1$ (mod p)

Proposition. $x^2 \equiv -1 \pmod{p}$ has a solution iff $p \equiv 1$ (mod 4)

Proof. By Wilson's,

$$\begin{aligned} -1 \equiv (p-1)! &\equiv (1)(2)\cdots\left(\frac{p-1}{2}\right)\left(-\frac{p-1}{2}\right)\cdots(-2)(-1) \\ &= (-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!^2 \end{aligned}$$

If $p \equiv 1$ mod 4, write $p = 4k+1$, and the RHS becomes $(2k!)^2$. But for $p \equiv -1$ (mod 4), ie. $p = 4k+3$, suppose we have some x st. $x^2 \equiv -1$ (mod p).

Then, by Fermat's, $x^p \equiv x \Rightarrow x^{p-1} \equiv 1$, and

$$\begin{aligned} 1 &\equiv x^{4k+2} \\ &= (x^2)^{2k+1} \\ &\equiv (-1)^{2k+1} \\ &= -1 \end{aligned}$$

Contradiction. □

x has order d (mod p), so d is the least positive integer st. $x^d \equiv 1$ (mod p). Suppose $x^k \equiv 1$ (mod p). Then $k > d$, so write $k = qd + r$ for $q > 0$, with remainder $r \in \{0, \cdots, d-1\}$.

Then

$$\begin{aligned} 1 = x^k &= x^{qd+r} \\ &= (x^d)^q x^r \\ &\equiv x^r \text{ (mod p)} \end{aligned}$$

ie $x^r \equiv 1$Since $r \in \{0, \cdots, d-1\}$, and d is the least positive integer st. $x^d \equiv 1$, we must have $r = 0$, and hence d divides k.

Now, suppose p is a prime factor of $F_n = 2^{2^n} + 1$. We want to determine the order of 2 (mod p), ie. the least positive integer d st. $2^d \equiv 1$ (mod p). Now, as p is a factor of F_n we have

$$\begin{aligned} 2^{2^n} + 1 &\equiv 0 \text{ (mod } p) \\ 2^{2^n} &\equiv -1 \text{ (mod } p) \end{aligned}$$

and by squaring both sides we have

$$2^{2^{n+1}} \equiv 1 \text{ (mod } p)$$

thus the order of 2 (mod p) divides 2^{n+1}.

I think the order is 2^{n+1} but don't know how to justify this. F_n and F_m are pairwise relatively coprime iff their gcd is 1.

Next, if p is of the form $4k+3$ and is a factor of some F_n, we have $\left(2^{2^{n-1}}\right)^2 \equiv -1$, but in the first part of the question we showed that x^2 only has a solution when p is of the form $4k+1$.

7D 2012

(i) CLAIM: $\sqrt{6}$ is irrational

Assume otherwise,

$$\sqrt{6} = \frac{p}{q}, \quad (p, q) = 1$$

Then $6q^2 = p^2 \Rightarrow 2|p^2$.

CLAIM: p^2 even $\Rightarrow$ p even.

Proof. Proof by contrapositive, if p not even, write $p = 2k + 1$ for some integer k. Then

$$\begin{aligned} p^2 &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2) + 1 \end{aligned}$$

Thus p^2 is not even. Hence p^2 even $\Rightarrow$ p even. □

Thus p even, and we can write $p = 2p'$ and $\sqrt{6} = \frac{2p'}{q} \Rightarrow 2|q$ also, which contradicts $(p, q) = 1$.

Now to show $\sqrt{2}+\sqrt{3}$ is irrational, all we need to do is assume it is rational and we get the following contradiction: then so is $(\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{6}$. But this is absurd since we have just showed $\sqrt{6}$ is irrational

(ii)

$$e := 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$$

Suppose is rational, $e = \frac{p}{q}$ for some integers p, q s.t. $(p, q) = 1$ Then $q!e \in \mathbb{N}$. But

$$q!e = \underbrace{q! + q! + \frac{q!}{2!} + \frac{q!}{3!} + \cdots + \frac{q!}{q!}}_{n} + \underbrace{\frac{q!}{(q+1)!} + \frac{q!}{(q+2)!} + \cdots}_{x},$$

where $n \in \mathbb{N}$ and

$$x = \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \cdots .$$

We can bound it by

$$0 < x < \frac{1}{q+1} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + \cdots = \frac{1}{q+1} \cdot \frac{1}{1 - 1/(q+1)} = \frac{1}{q}.$$

Now clearly $e > 2$, and

$$\begin{aligned} \frac{1}{2!} + \frac{1}{3!} + \cdots &< \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots \\ &< \frac{1/2}{1 - 1/2} = 1 \end{aligned}$$

Thus $2 < e < 3$, so $e = \frac{p}{q}$ is not an integer $\Rightarrow q > 1$. Hence

$$x < 5\frac{1}{q} < 1$$

Thus $q!e$ is the sum of an integer part n plus a non-integer part x. Contradiction.

(iii) Suppose the real root $x = \frac{p}{q}$, $(p, q) = 1$ Then

$$\begin{aligned} \frac{p^3}{q^3} + 4\frac{p}{q} - 7 = 0 &\Rightarrow \frac{p^3}{q} + 4pq - 7q^2 \\ &\Rightarrow \frac{p^3}{q} = 7q^2 - 4pq \end{aligned}$$

Then RHS is an integer $\Rightarrow$ LHS is an integer also, which contradicts the fact that $(p, q) = 1$.

(iv) Let $\log_2 3 = \frac{p}{q}$, $(p,q) = 1$ Now it must hold that

$$2^q = 3^p$$

which is nonsense as LHS is even, while the RHS is odd. Note this could be true if either p or q are equal to zero, but it is clear that this is not the case here.

8D 2012

Proposition. There is no injection from the power-set of $\mathbb{R}$ to $\mathbb{R}$

Proof.

- Suppose for the sake of contradiction that $f : \mathcal{P}(\mathbb{R}) \to \mathbb{R}$ is an injection.
- For each $t \in \mathrm{Im}(f)$, there exists a unique $s \in \mathcal{P}(\mathbb{R})$ st. $f(s) = t$. Define g as

$$g(t) = \begin{cases} s & \text{if } (t \in \operatorname{Im} f) \text{ and } (f(s) = t) \\ s_0 & \text{if } t \notin \operatorname{Im} f \end{cases}$$

  where s_0 is any element of S.

  By construction, given any $s \in S$ $\exists f(s) \in \mathbb{R}$ that maps to s under g, so $g : \mathbb{R} \to \mathcal{P}(R)$ is a surjection.
- Let $S = \{r \in \mathbb{R} : r \notin f(r)\}$. Since g is surjective, there must exist $r \in \mathbb{R}$ st. $g(r) = S$. If $r \in \mathbb{R}$, then $r \notin \mathbb{R}$ by the definition of S. Conversely if $r \notin S$, then $r \in S$.
- This is absurd, and we arrive at the conclusion that f cannot be an injection.

□

Proof. Suppose such an injection exists, $f : R \to \mathcal{P}(\mathbb{R})$. Take

$$S = \{r \in \mathbb{R} \ : \ r \notin f^{-1}(r)\}$$

where f^{-1} denotes the preimage of f. □

Proposition. There is an injection from $\mathbb{R}^2$ to $\mathbb{R}$

Proof. Let's construct an injective function $f : (0,1) \times (0,1) \to (0,1)$. Since there exist bijections between $\mathbb{R}$ and $(0,1)$ (eg. take $g(t) = (\tan t + \frac{\pi}{2})/2$), the proposed function f is sufficient to show such an injection exists.

Let the decimal representation of x be $0.x_1x_2x_3\cdots$, and that of y be $0.y_1y_2y_3\cdots$. Let $f(x,y)$ be $0.x_1y_1x_2y_2x_3y_3\cdots$

To make this function well-defined, avoid decimal representations that end with infinite successions of 9s. Then, f is injective. □

To specify some $f \in X := \{f : f(x) = x \text{ for all but finitely many } x \in \mathbb{R}\}$, I need

$$(r_1, f(r_1), r_2, f(r_2), \cdots, (r_n, f(r_n))$$

ie. a finite set of ordered pairs or reals, where the r_i represents the points at which the function is not the identity.

Given the number of ordered pairs $n \in \mathbb{N}$ we then encode these orders pairs as a member of the set $\mathbb{N} \times \mathbb{R}$, and inject this into $\mathbb{R}$:

$$N \times \mathbb{R} \to \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

Hence an injection $X \to \mathbb{R}$