Imperial College London

DEPARTMENT OF MATHEMATICS
IMPERIAL COLLEGE LONDON
Academic Year 2022-2023

Introduction to University Mathematics **MATH40001/MATH40009**

Solutions: Part II – Problem Sheet 1

1. (a) Suppose otherwise that 0 has predecessor $x \in \mathbb{N}$. Then we have by our definition of predecessor that $\sigma(x) = 0$. This contradicts Axiom P3.

   (b) Existence: We will use axiom P5. Define
$$S := \{x \in \mathbb{N} | x = 0 \text{ or } x \text{ has a predecessor in } \mathbb{N}\}.$$
By definition of S, $0 \in S$. We have to show next that if $n \in S$ then $\nu(n) \in S$. Assume $n \in S$. By definition of S, n is in $\mathbb{N}$ and $\nu(n) \in \mathbb{N}$, by Axiom P2, but then n is a predecessor of $\nu(n)$ by definition, hence $\nu(n) \in S$. Therefore $S = \mathbb{N}$ and if $n \in \mathbb{N}$, then either $n = 0$ or n has a predecessor.
Unicity: Assume $n_1, n_2 \in \mathbb{N}$, $n_1 \neq n_2$, two different predecessor of a number m, hence by definition $m = \nu(n_1) = \nu(n_2)$. By axiom 4, the function ν is injective, hence $\nu(n_1) = \nu(n_2)$ implies $n_1 = n_2$ which is a contradiction and yields the result.

   (c) By part b), for all $n \in \mathbb{N} - \{0\}$, there exists a $m \in \mathbb{N}$, such that $\pi(m) = n$, hence π is surjective, moreover the preimage is unique, and hence π is injective. Therefore π is bijective. The inverse function is exactly given by the modified successor function $\tilde{\nu} : \mathbb{N} \to \mathbb{N} - \{0\}$ with restricted image, since obviously $\tilde{\nu} \circ \pi(n) = \pi \circ \tilde{\nu}(n) = n$ on the appropriate domains of definition.

2. (a) Define
$$S = \{n \in \mathbb{N} | n \neq \nu(n)\}.$$
0 is trivially in S by axiom P3. Now assume $n \in S$. We want to show that $\nu(n) \in S$. But since ν is injective, if $n \neq \nu(n)$, then $\nu(n) \neq \nu^2(n)$ and therefore $\nu(n) \in S$ and finally $S = \mathbb{N}$, which means that our statement is true for all $n \in \mathbb{N}$.

   (b) Clearly $\mathbb{N} - \{0\}$ is a proper subset of $\mathbb{N}$. By definition, it is enough to find a bijection $f : \mathbb{N} \to \mathbb{N} - \{0\}$. We have found one in Question 1): This is exactly the predecessor function.

3. (a) Let A be the set $\{x \in \mathbb{N} \mid x + y = x \text{ implies } y = 0\}$. We have to show that $A = \mathbb{N}$. First suppose that $x = 0$. If $x + y = x$, then $0 + y = 0$ but $0 + y = y$, as proved in Lecture 1. So $y = 0$ (by transitivity of $=$). Thus $0 \in A$. Now suppose that $x \in A$. Then if $\nu(x) + y = \nu(x)$, we have $y + \nu(x) = \nu(x)$ by commutativity of addition. Then $\nu(y + x) = \nu(x)$ by the definition of addition. So $y + x = x$ by P3. Now applying commutativity again, we get $x + y = x$, and hence $y = 0$ by hypothesis. We conclude that $\nu(x) \in A$ as well. By P5, $A = \mathbb{N}$.

   (b) Note that, by commutativity, we only have to show that $x + y = 0$ implies $x = 0$. After all, given this, $x + y = 0$ implies $y + x = 0$, which implies $y = 0$.
So, let $A := \{y \in \mathbb{N} \mid x + y = 0 \text{ implies } x = 0\}$. Since $x + 0 = x$, we have that $x + 0 = 0$ implies $x = 0$. So $0 \in A$. Now suppose that $y \in A$. Suppose that $x + \nu(y) = 0$. Then $\nu(x + y) = 0$. This is impossible by P4. Thus $x + \nu(y) \neq 0$. It is then logically true that $x + \nu(y) \neq 0$ implies $x = 0$, since a false statement implies everything. Thus $\nu(y) \in A$ as well.

   (c) Let A be the set $A = \{x \in \mathbb{N} \mid x + y = y + x, \forall y \in \mathbb{N}$. We claim that $0 \in A$. By definition, $x + 0 = x$ for all $x \in \mathbb{N}$. As proved in Lecture 1, $0 = 0 + x$ as well. Therefore $0 \in A$.

Suppose that $x \in A$. Let $A_{\nu(x)}$ be the set $A_{\nu(x)} = \{y \in \mathbb{N} \mid \nu(x) + y = y + \nu(x)\}$. Note that $0 \in A_{\nu(x)}$, since $0 \in A$. Suppose that $y \in A_{\nu(x)}$. Then we have, using the definition of addition as well as $x \in A$:

$$\begin{aligned} \nu(x) + \nu(y) &= \nu(\nu(x) + y) = \nu(y + \nu(x)) = \nu(\nu(y + x)) \\ &= \nu(\nu(x + y)) = \nu(x + \nu(y)) = \nu(\nu(y) + x) = \nu(y) + \nu(x). \end{aligned} \quad (1)$$

Therefore also $\nu(y) \in A_{\nu(x)}$. By P5, we obtain that $A_{\nu(x)} = \mathbb{N}$. Therefore $\nu(x) \in A$. By P5 again, $A = \mathbb{N}$, and addition is commutative.

(d) Let $A = \{y \in \mathbb{N} \mid x \cdot y = y \cdot x, \forall x \in \mathbb{N}\}$. Given y, let $A_y := \{x \in \mathbb{N} \mid x \cdot y = y \cdot x\}$. Note that $y \in A$ if and only if $A_y = \mathbb{N}$. First we show that $0 \in A$. Note that $0 \cdot 0 = 0$ by definition, hence $0 \in A_0$. Suppose that $x \in A_0$. Then $0 \cdot \nu(x) = 0 \cdot x + 0 = 0 + 0 = 0$ by assumption and definition. But also $\nu(x) \cdot 0 = 0$ by definition. So $0 \cdot \nu(x) = \nu(x) \cdot 0$. So P5 implies $A_0 = \mathbb{N}$, hence $0 \in A$.

Now suppose that $y \in A$. We show that $A_{\nu(y)} = \mathbb{N}$. Note that $\nu(y) \cdot 0 = 0 \cdot \nu(y)$ since $0 \in A$. Now suppose that $\nu(y) \cdot x = x \cdot \nu(y)$. Then, using our assumptions, associativity of addition, (a), and definitions of addition and multiplication, we obtain:

$$\begin{aligned} \nu(y)\cdot\nu(x) &= \nu(y)\cdot x+\nu(y) = x\cdot\nu(y)+\nu(y) = x\cdot y+x+\nu(y) = y\cdot x+x+\nu(y) = y\cdot x+\nu(x+y) \\ &= y \cdot x + \nu(y + x) = y \cdot x + y + \nu(x) = y \cdot \nu(x) + \nu(x) = \nu(x) \cdot y + \nu(x) = \nu(x) \cdot \nu(y). \end{aligned} \quad (2)$$

4. (a) Note that $x \cdot 1 = x \cdot \nu(0) = x \cdot 0 + x = 0 + x = x$, using the definition of 1, of multiplication, and the property of addition by 0.

(b) Let $A = \{z \in \mathbb{N} \mid (x + y) \cdot z = x \cdot z + y \cdot z, \forall x, y \in \mathbb{N}\}$. Note that $0 \in A$ since $(x + y) \cdot 0 = 0 = 0 + 0 = x \cdot 0 + y \cdot 0$. Suppose that $z \in A$. Then, using associativity and commutativity of addition and definitions,

$$(x+y)\cdot\nu(z) = (x+y)\cdot z+(x+y) = x\cdot z+y\cdot z+x+y = (x\cdot z+x)+(y\cdot z+y) = x\cdot\nu(z)+y\cdot\nu(z).$$

Thus, by P5, $A = \mathbb{N}$.

(c) Let $A = \{z \in \mathbb{N} \mid (x\cdot y)\cdot z = x\cdot(y\cdot z) \forall x, y \in \mathbb{N}\}$. We have $(x\cdot y)\cdot 0 = 0$ and $x\cdot(y\cdot 0) = x\cdot 0 = 0$ by the preceding paragraph. Hence $0 \in A$. Now suppose that $z \in A$. Then

$$(x \cdot y) \cdot \nu(z) = (x \cdot y) \cdot z + (x \cdot y) = x \cdot (y \cdot z) + x \cdot y = x \cdot (y \cdot z + y) = x \cdot (y \cdot \nu(z)).$$

Here we used distributivity (on the right, which follows from (d) and (f)). Thus, by P5, $A = \mathbb{N}$.

5. Assume we have two function R and R', such that $R(0) = R'(0) = n_0$ and $R(\nu(n)) = \nu(R(n))$, $R'(\nu(n)) = \nu(R'(n))$. We have to show that $R(n) = R'(n)$ for all n. Let's define the set

$$S := \{n \in \mathbb{N} | R(n) = R'(n)\}.$$

For the value $n = 0$ we have obviously that $R(0) = R'(0)$. Now assume that $n \in S$, then $R(n) = R'(n)$. But $R(\nu(n)) = \nu(R(n)) = \nu(R'(n)) = R'(\nu(n))$ by definition and therefore $\nu(n) \in S$. Hence $S = \mathbb{N}$ and the functions R and R' coincide for all values and therefore are equal.

6. (a) Given $x \in \mathbb{N}$, let $A := \{y \in \mathbb{N} \mid y \leq x$ or $x \leq y\}$. Note that $0 \in A$ since $0 \leq x$, as $x = 0 + x$. Next, suppose $y \in A$. If $y \geq x$, i.e., $y = x + v$, then $\nu(y) = \nu(x + v) = x + \nu(v)$, which implies $\nu(y) \in A$. Suppose then that $y < x$. Then $x = y + v$. If $v = 0$ then $x = y$, a contradiction. So $v \neq 0$. Now, we proved in Question 1 that $v = \nu(v')$ for some $v' \in \mathbb{N}$. Then $x = y + \nu(v') = \nu(y + v') = \nu(y) + v'$. So also $y \leq x$. Therefore, we have shown that, in all cases, $y \in A$ implies $\nu(y) \in A$. By P5, $A = \mathbb{N}$.

i. Suppose that $a \neq 0$. Let $B = \{b \in \mathbb{N} \mid b = 0 \text{ or } a \cdot b \neq 0\}$. By definition, $0 \in B$. Suppose that $b \in B$. Then $a \cdot b \neq 0$. Now $a \cdot \nu(b) = a \cdot b + a \neq 0$ by 1c. So $\nu(b) \in B$, and $B = \mathbb{N}$ as desired.

ii. Suppose that $a \cdot b = a$ and $a \neq 0$. Then $b \neq 0$, otherwise $a \cdot b = 0$ and $a = 0$, a contradiction. So also $b \neq 0$. Since again by Question 1, $b = \nu(b')$ for some b'. Then $a \cdot b = a \cdot b' + a = a$. Moreover $a \cdot b' = 0$. By part i) and $a \neq 0$, we get $b' = 0$. Then $b = \nu(b') = 1$.

iii. Suppose $a \cdot b = 1$. Then $a, b \neq 0$, since $0 \neq 1$ (as 0 is not a successor but 1 is). Now, as before, we have $a = \nu(a')$, and similarly $b = \nu'(b)$. So $a \cdot b = \nu(a') \cdot \nu(b') = \nu(a') \cdot b' + \nu(a') = \nu(\nu(a') \cdot b' + a') = 1 = \nu(0)$. Hence $\nu(a') \cdot b' + a' = 0$ by the injectivity of ν. Therefore by a result proved previously, $a' = 0$, so $a = \nu(a') = 1$. By commutativity, also $b \cdot a = 1$, and we also then conclude that $b = 1$. So $a = b = 1$ as desired.

iv. Reflexivity: note that $x \mid x$ since $x = x \cdot 1$.
Transitivity: Suppose that $x \mid y$ and $y \mid z$. Write $y = x \cdot a$ and $z = y \cdot b$. Then $z = (x \cdot a) \cdot b = x \cdot (a \cdot b)$, by associativity. Then $x \mid z$.
Antisymmetry: Suppose that $x \mid y$ and $y \mid x$. Then we have $y = x \cdot a$ and $x = y \cdot b$, for some integers a and b hence $x = x \cdot (a \cdot b)$. Suppose first that $x = 0$. Then $y = x \cdot a$ implies also $y = 0$. Then $x = y$. Next suppose that $x \neq 0$. Then $y \neq 0$, otherwise $x = y \cdot b$ would yield $x = 0$, a contradiction. Next $x = x \cdot (a \cdot b)$ implies, by part iii), that $a \cdot b = 1$. By part iii) again, we get $a = b = 1$. Then $x = y$, as desired.

7. (a) First note that $(n-1)(n+1) = (n-1)n + (n-1)1 = n^2 - n + n - 1 = n^2 - 1$. Next if n is odd, then $n-1$ and $n+1$ are consecutive even natural numbers. Now suppose that $4 \mid n-1$. Since $n+1$ is even, $2 \mid n+1$. We get $4 \cdot 2 \mid (n-1)(n+1) = n^2 - 1$, which is what we wanted. Next suppose that $4 \nmid n-1$. Since $2 \mid n-1$, we have $n-1 = 2k$ for some k. Since $4 \nmid n-1$, k must be odd. Then $n+1 = 2(k+1)$ and $k+1$ is even. Hence $4 \mid n+1$, and again we have $2 \cdot 4 \mid (n-1)(n+1) = n^2 - 1$. In any case, $8 \mid n^2 - 1$.

(b) Note that $b > 1$ implies that $b = 1 + v$ for some $v \in \mathbb{N}$. Since $b \neq 1$, we have $v \neq 0$. Then $ab = a \cdot 1 + a \cdot v = a + a \cdot v$. Since $a, v \neq 0$, by Part i), we have $a \cdot v \neq 0$. So $ab \geq a$ and $ab \neq a$, which gives the desired result.

(c) Let $n > 1$. Let $A = \{m \in \mathbb{N} \mid m > 1 \text{ and } m \mid a\}$. By the well ordering property, there is a smallest $d \in A$. Suppose that d is not prime. By definition, also $d > 1$, and since $1 > 0$, also $d \neq 0$. So $d = d_1 \cdot d_2$ for $d_1, d_2 \neq d$ and $d_1, d_2 > 1$. Then by transitivity of divisibility, $d_1, d_2 \mid n$ as well. By Part b), $d_1 < d$, which is a contradiction. So d was prime.

8. (a) Let $A := \{m \in \mathbb{N} \mid \text{ it is possible to make } m \text{ cents using } 2 \text{ and } 3 \text{ cent stamps}\} \cup \{0, 1\}$. We need to show that $A = \mathbb{N}$. First, $0, 1, 2, 3 \in A$ is obvious. Now suppose that $A \neq \mathbb{N}$. Let $b \in \mathbb{N} \setminus A$ be the least element not in A. If $b \leq 3$ we have a contradiction as we are in A (note that $b \leq 3$ implies $b = 0$ or $b = \nu(b') = b' + 1$ with $b' + 1 \leq 3 \Rightarrow b' \leq 2$, since we know the contrapositive $b' > 2 \Rightarrow b' + 1 > 3$). Suppose then that $b > 3$. Then $b - 2 > 1$. But also $b - 2 < b$. So $b - 2 \in A$. But then we can form $b - 2$ with 2 and 3 cent stamps, then add a 2 cent stamp to make b. This contradicts that $b \notin A$.

(b) Let d be the least element of X (using the well-ordering principle). We claim that $X = \{d, 2d, 3d, \ldots\}$. First we prove "$\supseteq$". We have $1 \cdot d \in X$. Suppose that $n \cdot d \in X$. Then $n \cdot d + d = (n+1) \cdot d \in X$, by (2). By induction, $n \cdot d \in X$ for all n.

Next we show "$\subseteq$". Suppose not. Then let $m \in X$ be minimal such that it is not a multiple of d (using the well-ordering principle). Since $d \in X$ is minimal, and $m \neq d$, we have $m > d$. Then by (3), we also have $m - d \in X$. This is, however, also not a multiple of d: $m - d = d \cdot k$ would imply $m = d \cdot (k+1)$, a contradiction. But this contradicts the minimality of d. This establishes the inclusion.

Finally we have to show that d is unique. Indeed, $X = \{d, 2d, 3d, \ldots\}$ certainly implies that d is the least element of X, since $1 \cdot d \leq m \cdot d$ for all $1 \leq m$. This uniquely characterises d.