X-MA2C01-1: Partial Worked Solutions

David R. Wilkins

May 2013

1. (a) *Let A, B and C be sets. Prove that*

$$(A \setminus (B \cup C)) \cup (B \setminus C) = (A \cup B) \setminus C.$$

[Venn Diagrams, by themselves without an accompanying logical argument, do not provide sufficient justification to constitute a proof of the result.]

[8 marks]

Let $x \in (A \setminus (B \cup C)) \cup (B \setminus C)$. Then either $x \in (A \setminus (B \cup C)$ or else $x \in B \setminus C$. If $x \in (A \setminus (B \cup C)$ then $x \in A$ and also $x \notin C$ and therefore $x \in (A \cup B) \setminus C$. If $x \in B \setminus C$ then $x \in B$ and $x \notin C$, and therefore $x \in (A \cup B) \setminus C$. Thus each element x of $(A \setminus (B \cup C)) \cup (B \setminus C)$ is an element of $(A \cup B) \setminus C$.

Now let $x \in (A \cup B) \setminus C$. Then $x \notin C$. We consider separately the case when, in addition, $x \in B$ and the case when $x \notin B$. If $x \in B$ then $x \in B \setminus C$ and therefore $x \in (A \setminus (B \cup C)) \cup (B \setminus C)$. If $x \notin B$ then also $x \in A$ (because $x \in A \cup B$) and $x \notin C$ and therefore $x \notin B \cup C$, hence $x \in A \setminus (B \cup C)$, hence $x \in (A \setminus (B \cup C)) \cup (B \setminus C)$. Thus each element x of $(A \cup B) \setminus C$ is an element $(A \setminus (B \cup C)) \cup (B \setminus C)$.

Because each element of one of the two sets is an element of the other, we conclude that

$$(A \setminus (B \cup C)) \cup (B \setminus C) = (A \cup B) \setminus C,$$

as required.

(b) *Let Q denote the relation on the set $\mathbb{Z}$ of integers, where integers x and y satisfy xQy if and only if both $x \leq y + 3$ and $y \leq x + 3$. Determine whether the relation Q is*

(i) reflexive,

(ii) symmetric,
(iii) transitive,
(iv) anti-symmetric,
(v) an equivalence relation,
(vi) a partial order,

[Give appropriate short proofs and/or counterexamples to justify your answers.]

[12 marks]

(i) The relation Q on $\mathbb{Z}$ is reflexive. Indeed $x \leq x+3$ and therefore xQx for all integers x.

(ii) The relation Q is symmetric. Integers x and y satisfy yQx if and only if $y \leq x+3$ and $x \leq y+3$, and this is the case if and only if xQy.

(iii) The relation Q is not transitive. For example, $1Q3$ and $3Q5$, but $1 \not{Q} 5$.

(iv) The relation Q is not anti-symmetric. For example, $1Q2$ and $2Q1$ but $1 \neq 2$.

(v) The relation Q is not an equivalence relation because it is not transitive.

(vi) The relation Q is not a partial order because it is not transitive, and also because it is not anti-symmetric.

2. (a) *Let $f\colon \mathbb{R} \to \mathbb{R}$ be the function from the set $\mathbb{R}$ of real numbers to itself defined such that*

$$f(x) = \begin{cases} \dfrac{1}{x} & \textit{if } x > 1; \\ x & \textit{if } x \leq 1. \end{cases}$$

Determine whether or not this function is injective, whether or not it is surjective, and whether or not it is invertible, giving brief reasons for your answers.

[8 marks]

The function is not injective. Indeed $f(2) = f(\frac{1}{2}) = \frac{1}{2}$. Thus distinct elements of the domain do not always get mapped to distinct elements of the codomain.

The function is not surjective, because $f(x) \leq 1$ for all real number x. Thus, for example, 2 belongs to the codomain of the function, but does not belong to the range.

Because the function is neither injective or surjective, it cannot be invertible.

(b) *Let X denote the set of odd integers, and let $\otimes$ be the binary operation on X defined such that $x \otimes y = \frac{1}{2}(xy + 3x + 3y + 3)$ for all odd integers x and y. Prove that $(X, \otimes)$ is a monoid. What is the identity element of this monoid? Determine the inverse of each invertible element of $(X, \otimes)$. Is $(X, \otimes)$ a group?*

[12 marks]

In order to prove that $(X, \otimes)$ is a monoid, we must show that the binary operation $\otimes$ is associative, and also that there exists an identity element for this binary operation belonging to the set X. Let $x, y, z \in X$. Then

$$\begin{aligned}
(x \otimes y) \otimes z &= \left(\frac{1}{2}(xy + 3x + 3y + 3)\right) \otimes z \\
&= \frac{1}{2}\left(\frac{1}{2}(xy + 3x + 3y + 3)z + \frac{3}{2}(xy + 3x + 3y + 3) + 3z + 3\right) \\
&= \frac{1}{4}\left(xyz + 3xz + 3yz + 3z + 3xy + 9x + 9y + 9 + 6z + 6\right) \\
&= \frac{1}{4}\left(xyz + 3(xz + yz + xy) + 9(z + x + y) + 15\right),
\end{aligned}$$

$$\begin{aligned}
x \otimes (y \otimes z) &= x \otimes \left(\frac{1}{2}(yz + 3y + 3z + 3)\right) \\
&= \frac{1}{2}\left(\frac{1}{2}x(yz + 3y + 3z + 3) + 3x + \frac{3}{2}(yz + 3y + 3z + 3) + 3\right) \\
&= \frac{1}{4}\left(xyz + 3xy + 3xz + 3x + 6x + 3yz + 9y + 9z + 9 + 6\right) \\
&= \frac{1}{4}\left(xyz + 3(xy + xz + yz) + 9(x + y + z) + 15\right) \\
&= (x \otimes y) \otimes z.
\end{aligned}$$

Thus the binary operation $\otimes$ is associative. An element x of X is an identity element for the binary operation if and only if $x \otimes e = e \otimes x = x$ for all $x \in X$, i.e., if and only if

$$\frac{1}{2}(xe + 3x + 3e + 3) = x$$

for all odd integers x. But

$$\begin{aligned}
\frac{1}{2}(xe+3x+3e+3) &= x \\
\iff xe+3x+3e+3 &= 2x \\
\iff xe+x+3e+3 &= 0 \\
\iff (x+3)(e+1) &= 0.
\end{aligned}$$

It follows that -1 is an identity element for the binary operation $\otimes$ on X. An element y of X if the inverse of an element x of X if and only if

$$\frac{1}{2}(xy+3x+3y+3) = -1.$$

Now

$$\begin{aligned}
\frac{1}{2}(xy+3x+3y+3) &= -1 \\
\iff xy+3x+3y+3 &= -2 \\
\iff (x+3)(y+3) &= 4.
\end{aligned}$$

But x and y are odd integers, and therefore $x+3$ and $y+3$ are even integers, and thus $(x+3)(y+3)$ is divisible by 4 for all $x, y \in X$. It follows that an odd integer x is invertible if and only if $x+3 = \pm 2$, in which case x is its own inverse. Thus -1 and -5 are invertible, and are their own inverses.

3. (a) *Describe the formal language over the alphabet $\{0,1\}$ generated by the context-free grammar whose non-terminals are $\langle S\rangle$ and $\langle A\rangle$, whose start symbol is $\langle S\rangle$ and whose productions are the following:*

$$\begin{aligned}
\langle S\rangle &\to 0\langle A\rangle \\
\langle A\rangle &\to 101\langle S\rangle \\
\langle S\rangle &\to \varepsilon
\end{aligned}$$

(where ε denotes the empty word). Is this context-free grammar a regular grammar?

[6 marks]

The language generated by this grammar is the language

$$\varepsilon,\ 0101,\ 01010101,\ 010101010101,\ 0101010101010101, \ldots$$

consisting of those strings consisting of zero or more repetitions of the substring 0101.

The grammar is not a regular grammar because the production $\langle A\rangle \rightarrow 101\langle S\rangle$ is of a type that is not permitted in a regular grammar.

(b) *Give the specification of a finite state acceptor that accepts the language over the alphabet* $\{a, c, g, t\}$ *consisting of all strings made up of letters from this alphabet (including the empty string) that do not contain the substring 'cat'.*

In particular you should specify the set of states, the starting state, the finishing states, and the transition table that determines the transition function of the finite state acceptor.

[8 marks]

States: S, A, B, E.

Starting state: S.

Finishing states: S, A, B.

Transition table:

	a	c	g	t
S	S	A	S	S
A	B	A	S	S
B	S	A	S	E
E	E	E	E	E

(Note that the machine is in state A if and only if the last character entered was 'c' and not error has previously occurred, and that the machine is in state B if and only if the last two characters entered were 'c' followed by 'a' and no error has previously occurred. It is an error to enter the character t when the machine is in state B. Any character can be entered without producing an error whenever the machine is in state S or state A.)

(c) *Devise a regular context-free grammar to generate the language over the alphabet* $\{a, c, g, t\}$ *described above in (b).*

[6 marks]

Start symbol: $\langle S\rangle$.

Productions:

$$
\begin{aligned}
\langle S\rangle &\rightarrow a\langle S\rangle\\
\langle S\rangle &\rightarrow c\langle A\rangle\\
\langle S\rangle &\rightarrow g\langle S\rangle\\
\langle S\rangle &\rightarrow t\langle S\rangle\\
\langle S\rangle &\rightarrow \varepsilon\\
\langle A\rangle &\rightarrow a\langle B\rangle\\
\langle A\rangle &\rightarrow c\langle A\rangle\\
\langle A\rangle &\rightarrow g\langle S\rangle\\
\langle A\rangle &\rightarrow t\langle S\rangle\\
\langle A\rangle &\rightarrow \varepsilon\\
\langle B\rangle &\rightarrow a\langle S\rangle\\
\langle B\rangle &\rightarrow c\langle A\rangle\\
\langle B\rangle &\rightarrow g\langle S\rangle\\
\langle B\rangle &\rightarrow \varepsilon
\end{aligned}
$$

4. In this question, all graphs are undirected graphs.

(a)

(i) What is meant by saying that a graph is regular*?*

(ii) What is an Eulerian circuit *in a graph?*

(iii) What is a Hamiltonian circuit *in a graph?*

(iv) What is meant by saying that a graph is a tree*?*

(v) Give the definition of an isomorphism *between two undirected graphs.*

[7 marks]

(i) The graph is *regular* if all vertices have the same degree.

(ii) An *Eulerian circuit* is a circuit that traverses all edges of the graph exactly once.

(iii) A *Hamiltonian circuit* is a circuit that passes through all vertices exactly once before returning to its starting point.

(iv) A graph is a *tree* if it is connected and it has no circuits.

(v) An *isomorphism* between two graphs is an invertible function from the set of vertices of the first graph to the set of vertices of the second graph with the property that two vertices of the first graph are joined by an edge if and only if the corresponding vertices of the second graph are joined by an edge.

(b) *Let G be the undirected graph whose vertices are a, b, c, d and e and whose edges are the following:*

$$a\,b, \quad a\,e, \quad b\,c, \quad b\,e, \quad c\,d, \quad c\,e, \quad d\,e.$$

(i) Is this graph regular?

(ii) Does this graph have an Eulerian circuit?

(iii) Does this graph have a Hamiltonian circuit?

(iv) Is this graph a tree?

[Give brief reasons for each of your answers.]

[8 marks]

(i) The graph is not regular. The vertices do not all have the same degree, vertices a and d are of degree 2, vertices b and c are of degree 3 and vertex e is of degree 4.

(ii) If a graph has an Eulerian circuit then all vertices must be of even degree. The vertices b and c have degree 3. Therefore this graph cannot have an Eulerian circuit.

(iii) The graph has a Hamiltonian circuit. One such is $a\,b\,c\,d\,e\,a$.

(iv) The graph is not a tree because it has circuits. Indeed $a\,b\,e\,a$ is a circuit (as is the Hamiltonian circuit given above).

(c) *Let V denote the set of vertices of the graph G defined in (b). Determine all possible isomorphisms $\varphi\colon V \to V$ from the graph G to itself that satisfy $\varphi(b) = c$.*

[5 marks]

There is only one isomorphism $\varphi colon V \to V$, and it satisfies

$$\varphi(a) = d,\ \ \varphi(b) = c,\ \ \varphi(c) = b,\ \ \varphi(d) = a,\ \ \varphi(e) = e,\ \ .$$

An isomorphism $\varphi\colon V \to V$ must be invertible. Moreover $\deg \varphi(v) = \deg v$ for all $v \in V$. Therefore $\varphi(e) = e$, since e is the only vertex of degree 4. Now $\varphi(c)$ must be a vertex of degree 3, but it cannot be the vertex c, and therefore $\varphi(c) = b$. Also $\varphi(a)$ must be a vertex of degree 2 adjacent to $\varphi(b)$, and thus adjacent to the vertex c, and therefore $\varphi(a) = d$, and similarly $\varphi(d) = a$.

5. (a) *Any function y of a real variable x that solves the differential equation*

$$\frac{d^4y}{dx^4} - 16y = 0$$

may be represented by a power series of the form

$$y = \sum_{n=0}^{+\infty} \frac{y_n}{n!} x^n,$$

where the coefficients $y_0, y_1, y_2, y_3, \ldots$ of this power series are real numbers.

Find values of these coefficients y_n for $n = 0, 1, 2, 3, 4, \ldots$ that yield a solution to the above differential equation with $y_0 = 1$, $y_1 = 0$, $y_2 = -4$ and $y_3 = 0$.

[8 marks]

$$\frac{d^4y}{dx^4} - 16y = \sum_{n=0}^{+\infty} \frac{y_{n+4} - 16y_n}{n!} x^n.$$

It follows that the function y of x satisfies the differential equation if and only if $y_{n+4} = 16y_n$ for all non-negative integers n. Now $16 = 2^4$. It follows that the y_n must satisfy

$$y_n = \begin{cases} 2^n & \text{if } n \equiv 0 \text{ mod. } 4; \\ -2^n & \text{if } n \equiv 2 \text{ mod. } 4; \\ 0 & \text{if } n \text{ is odd.} \end{cases}$$

(b) *Find the general solution of the differential equation*

$$\frac{d^2y}{dx^2} - 6\frac{dy}{dx} + 25y = \cos 5x.$$

[12 marks]

The general solution of the differential equation has the form $y = y_P + y_C$ where y_P is a particular integral, and where y_C is a complementary function satisfying the associated homogeneous differential equation $y_C'' - 6y_C' + 25y_C = 0$. The auxiliary polynomial $s^2 - 6s + 25$ has roots $3 \pm 4i$, where $i = \sqrt{-1}$. (Indeed the sum of these roots is 6 and the product is 25.) Therefore

$$y_C = e^{3x}(A \cos 4x + B \sin 4x).$$

We look for a particular integral of the form

$$y_P = p\cos 5x + q\sin 5x,$$

where p and q are constants to be determined. Now

$$\begin{aligned} y_P &= p\cos 5x + q\sin 5x, \\ y_P' &= 5q\cos 5x - 5p\sin 5x, \\ y_P'' &= -25p\cos 5x - 25q\sin 5x, \end{aligned}$$

and therefore

$$y_P'' - 6y_P' + 25y_P = -30q\cos 5x + 30p\sin 5x.$$

Therefore we must take $p = 0$ and $q = -\frac{1}{30}$. Thus the general solution to the differential equation is

$$y = -\frac{1}{30}\cos 5x + e^{3x}(A\cos 4x + B\sin 4x).$$

6. (a) *Let $(z_n : n \in \mathbb{Z})$ be a doubly-infinite 3-periodic sequence of complex numbers (which thus has the property that $z_{n+3} = z_n$ for all integers n). Also let $\omega = \exp(2\pi i/3) = \frac{1}{2}(-1+\sqrt{3}\, i)$, where $i = \sqrt{-1}$. Prove that*

$$z_j = c_0 + c_1\omega^j + c_2\omega^{2j}$$

for all integers j, where

$$c_0 = \frac{1}{3}(z_0+z_1+z_2), \quad c_1 = \frac{1}{3}(z_0+z_1\omega^2+z_2\omega), \quad c_2 = \frac{1}{3}(z_0+z_1\omega+z_2\omega^2).$$

[Note that $1+\omega+\omega^2 = 0$ and $\omega^3 = 1$. You should give a direct proof that utilizes these properties of the complex number ω, and does not merely claim the result of any more general theorem stated in the lecture notes.]

[12 marks]

Note that

$$z_{j+3} = c_0 + c_1\omega^j\omega^3 + c_2\omega^{2j}\omega^6 = c_0 + c_1\omega^j + c_2\omega^{2j} = z_j$$

for all integers j. Therefore the sequence $(z_n : n \in \mathbb{Z})$ is 3-periodic. It therefore suffices to verify that the required identity holds for $j = 0$, $j = 1$ and $j = 2$.

Now

$$
\begin{aligned}
c_0 + c_1 + c_2 &= \frac{1}{3}\left(3z_0 + z_1(1+\omega^2+\omega) + z_2(1+\omega+\omega^2)\right) \\
&= z_0, \\
c_0 + c_1\omega + c_2\omega^2 &= \frac{1}{3}\Bigg(z_0(1+\omega+\omega^2) + z_1(1+\omega^2\omega+\omega\omega^2) \\
&\qquad + z_2(1+\omega\omega+\omega^2\omega^2)\Bigg) \\
&= \frac{1}{3}\Bigg(z_0(1+\omega+\omega^2) + 3z_1 + z_2(1+\omega^2+\omega)\Bigg) \\
&= z_1, \\
c_0 + c_1\omega^2 + c_2\omega^4 &= \frac{1}{3}\Bigg(z_0(1+\omega^2+\omega^4) + z_1(1+\omega^2\omega^2+\omega\omega^4) \\
&\qquad + z_2(1+\omega\omega^2+\omega^2\omega^4)\Bigg) \\
&= \frac{1}{3}\Bigg(z_0(1+\omega+\omega^2) + z_1(1+\omega+\omega^2) + 3z_2\Bigg) \\
&= z_2.
\end{aligned}
$$

The result follows.

(b) *Let $(z_n : n \in \mathbb{Z})$ be the doubly-infinite 3-periodic sequence with $z_0 = 1$, $z_1 = 2$ and $z_2 = -2$. Find values of c_0, c_1 and c_2 such that*

$$z_n = c_0 + c_1\omega^n + c_2\omega^{2n}$$

for all integers n, where $\omega = e^{2\pi i/3}$.

[8 marks]

$$
\begin{aligned}
c_0 &= \frac{1}{3}(z_0+z_1+z_2) = \frac{1}{3} \\
c_1 &= \frac{1}{3}(z_0+z_1\omega^2+z_2\omega) = \frac{1}{3}(1+2\omega^2-2\omega) = \frac{1}{3}(1-2\sqrt{3}\,i) \\
c_2 &= \frac{1}{3}(z_0+z_1\omega+z_2\omega^2) = \frac{1}{3}(1+2\omega-2\omega^2) = \frac{1}{3}(1+2\sqrt{3}\,i),
\end{aligned}
$$

because

$$\omega - \omega^2 = -\frac{1}{2} + \frac{\sqrt{3}\,i}{2} - \left(-\frac{1}{2} - \frac{\sqrt{3}\,i}{2}\right) = \frac{2\sqrt{3}\,i}{2}.$$

7. (a) *Find the lengths of the vectors* $(4, 1, 2)$ *and* $(2, 2, 2)$ *and also the cosine of the angle between them.*

[6 marks]

Let $\mathbf{v} = (4, 1, 2)$ and $\mathbf{w} = (2, 2, 2)$. The lengths of these vectors are given by

$$\begin{aligned} |\mathbf{v}| &= \sqrt{4^2 + 1^2 + 2^2} = \sqrt{21} \\ |\mathbf{w}| &= \sqrt{2^2 + 2^2 + 2^2} = \sqrt{12}. \end{aligned}$$

The scalar product $\mathbf{v}.\mathbf{w}$ of these vectors is given by

$$\mathbf{v}.\mathbf{w} = 4 \times 2 + 1 \times 2 + 2 \times 2 = 14.$$

The cosine $\cos\theta$ of the angle θ between these vectors is thus

$$\begin{aligned} \cos\theta &= \frac{\mathbf{v}.\mathbf{w}}{|\mathbf{v}|\,|\mathbf{w}|} = \frac{14}{\sqrt{21} \times \sqrt{12}} = \frac{14}{\sqrt{3} \times \sqrt{7} \times 2 \times \sqrt{3}} = \frac{14}{6\sqrt{7}} \\ &= \frac{\sqrt{7}}{3} \approx 0.881917. \end{aligned}$$

(b) *Find the components of a non-zero vector that is orthogonal to the two vectors* $(3, 2, 5)$ *and* $(2, 1, 7)$*, and determine the equation of the plane in* $\mathbb{R}^3$ *that contains the points* $(3, 4, 6)$*,* $(6, 6, 11)$ *and* $(5, 5, 13)$*.*

[8 marks]

Calculating the vector product of the two given vectors, we find that

$$\begin{aligned} (3, 2, 5) \times (2, 1, 7) &= (2 \times 7 - 5 \times 1, 5 \times 2 - 3 \times 7, 3 \times 1 - 2 \times 2) \\ &= (9, -11, -1) \end{aligned}$$

Thus $(9, -11, -1)$ is a non-zero vector that is orthogonal to the two given vectors. (Note that the scalar product of $(9, -11, -1)$ with each of the two given vectors is equal to zero.)

Now the vector $(3, 2, 5)$ is the displacement vector from $(3, 4, 6)$ to $(6, 6, 11)$, and $(2, 1, 7)$ is the displacement vector from $(3, 4, 6)$ to $(5, 5, 13)$. Therefore the plane through the three given points is perpendicular to the vector $(9, -11, -1)$ and therefore is specified by an equation of the form

$$9x - 11y - z = k$$

for some constant k. Moreover

$$k = 9 \times 3 - 11 \times 4 - 6 = -23.$$

Thus the equation of the plane is

$$9x - 11y - z = -23.$$

(c) *Let the quaternions q and r be defined as follows:*

$$q = i - 2k, \quad r = 1 - j + 5k.$$

Calculate the quaternion products qr and rq. [Hamilton's basic formulae for quaternion multiplication state that

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.]$$

[6 marks]

$$\begin{aligned}
qr &= (i - 2k)(1 - j + 5k) = i(1 - j + 5k) - 2k(1 - j + 5k) \\
&= i - ij + 5ik - 2k + 2kj - 10k^2 = i - k - 5j - 2k - 2i + 10 \\
&= 10 - i - 5j - 3k \\
rq &= (1 - j + 5k)(i - 2k) = (1 - j + 5k)i - (1 - j + 5k)2k \\
&= i - ji + 5ki - 2k + 2jk - 10k^2 = i + k + 5j - 2k + 2i + 10 \\
&= 10 + 3i + 5j - k
\end{aligned}$$

8. (a) *Find an integer x such that $x \equiv 5$ (mod. 7), $x \equiv 2$ (mod. 17) and $x \equiv 3$ (mod. 19).*

[12 marks]

$17 \times 19 = 323$, $7 \times 19 = 133$, $7 \times 17 = 119$. 323 mod. $7 = 1$, 133 mod. $17 = 14$, 119 mod. $19 = 5$.

Let $u_1 = 323$. Then $u_1 \equiv 1$ (mod. 7), $u_1 \equiv 0$ (mod. 17), $u_1 \equiv 0$ (mod. 19).

Now $11 \times 14 = 154$ and $154 \equiv 1$ (mod. 17), therefore $11 \times 133 \equiv 1$ (mod. 17). Now $11 \times 133 = 1463$. Let $u_2 = 1463$. Then $u_2 \equiv 0$ (mod. 7), $u_2 \equiv 1$ (mod. 17), $u_2 \equiv 0$ (mod. 19).

Now $4 \times 5 = 20$ and $20 \equiv 1$ (mod. 19), therefore $4 \times 119 \equiv 1$ (mod. 19). Now $4 \times 119 = 476$. Let $u_3 = 476$. Then $u_3 \equiv 0$ (mod. 7), $u_3 \equiv 0$ (mod. 17), $u_3 \equiv 1$ (mod. 19).
Let

$$\begin{aligned} x &= 5u_1 + 2u_2 + 3u_3 \\ &= 5 \times 323 + 2 \times 1463 + 3 \times 476 \\ &= 1615 + 2926 + 1428 \\ &= 5969 \end{aligned}$$

Then x satisfies the required congruences. Any two solutions differ by a multiple of 2261, because 7, 17 and 19 are pairwise coprime and $2261 = 7 \times 17 \times 19$. Thus the following integers satisfy the required simultaneous congruences:

$$1447, \quad 3708, \quad 5969, \quad 8230, \quad 10491.$$

(b) *Find the value of the unique integer x satisfying $0 \leq x < 17$ for which*

$$4^{1024000000002} \equiv x \ (\text{ mod. } 17).$$

[8 marks]

$$\begin{aligned} 4 &\equiv 1 \text{ (mod. 17)} \\ 4^2 &\equiv 16 \text{ (mod. 17)} \\ 4^3 &\equiv 13 \text{ (mod. 17)} \\ 4^4 &\equiv 1 \text{ (mod. 17)} \\ 4^5 &\equiv 16 \text{ (mod. 17)} \\ &\vdots \end{aligned}$$

It follows that $4^{4k} \equiv 1$ (mod. 17) for all non-negative integers k. Now 1024000000000 is divisible by 4. Therefore $4^{1024000000000} \equiv 1$ (mod. 17), and therefore $4^{1024000000002} \equiv 4^2 \equiv 16$ (mod. 17).