Solutions #4

1. Consider the integer \( A = 4444^{4444} \). Let \( B \) denote the sum of the digits of \( A \), let \( C \) denote the sum of the digits of \( B \), and let \( D \) denote the sum of the digits of \( C \). Find \( D \).

Solution. We start with the following (well-known) fact:

Lemma. Let \( N \) be a positive integer with decimal expansion \( a_k a_{k-1} \ldots a_1 a_0 \) and let \( M = a_0 + a_1 + \cdots + a_k \) be the sum of the digits of \( N \). Then \( N \equiv M \pmod{9} \).

Proof of the Lemma. Since \( 10 \equiv 1 \pmod{9} \), for any \( j \in \mathbb{Z}_{\geq 0} \), we have \( 10^j \equiv 1 \pmod{9} \).

Thus
\[
N = a_k a_{k-1} \ldots a_1 a_0 = \sum_{j=0}^{k} a_j 10^j \equiv \sum_{j=0}^{k} a_j = M \pmod{9}.
\]

As a consequence of the Lemma we conclude that \( A \equiv B \equiv C \equiv D \pmod{9} \). To compute the congruence class of \( A \mod 9 \) we calculate that
\[
4444 \equiv 4 + 4 + 4 + 4 = 16 \equiv 7 \pmod{9}.
\]

Furthermore,
\[
7^3 \equiv (-2)^3 = -8 \equiv 1 \pmod{9}.
\]

Moreover, \( 4444 \equiv 1 \pmod{3} \) (Why?) and hence \( 4444 = 3q + 1 \). With this in mind we obtain
\[
A = 4444^{4444} \equiv 7(3q + 1) = (7^3)^q \times 7 \equiv 1^q \times 7 = 7 \pmod{9}.
\]

Of course, this also means that \( D \equiv 7 \pmod{9} \), i.e., \( D = 7 + 9t \) for some \( t \in \mathbb{Z}_{\geq 0} \).

The next step is to estimate \( D \). Since \( A = 4444^{4444} < 10000^{4444} = 10^{3 \times 4444} \), we conclude that \( A \) has fewer than \( 3 \times 4444 \) digits. Hence \( B < 9 \times (3 \times 4444) < 10 \times 3 \times 5000 = 150000 \). In particular, \( B \) has 6 digits or fewer. Hence \( C \leq 9 \times 6 = 54 \). The largest sum of digits for a number no greater than 54 is 13 = 4 + 9, attained for the integer 49. Hence \( D \leq 13 \).

Combining \( D = 7 + 9t \) for some \( t \in \mathbb{Z}_{\geq 0} \) with \( D \leq 13 \) we conclude that \( D = 7 \).

\( \square \)

2. Solve the following equations:

(a) \( 7x = 2 \) in \( \mathbb{Z}_{24} \);
(b) \( 34x = 14 \) in \( \mathbb{Z}_{51} \);
(c) \( 15x = 5 \) in \( \mathbb{Z}_{65} \).

Solution. To solve these equations, we reduce the equation
(1) \( ax = b \) in \( \mathbb{Z}_m \)
first to the equation
(2) \( ax \equiv b \pmod{m} \)
and finally to the equation
(3) \( ax - b = mq \) or, equivalently, \( ax - mq = b \),
which we know how to solve.

In performing these reductions, we should keep in mind what the meaning of the variables in each of the equations above is. In (1), \( a, x, \) and \( b \) are elements of \( \mathbb{Z}_m \). Strictly speaking, \( 7x = 2 \) in \( \mathbb{Z}_{24} \) should be written as \([7]_{24}x = [2]_{24}\). In both (2) and (3), \( a, x, \) and \( b \) are integers. As a consequence, once we find the solutions of (3), we need to reduce them modulo \( m \) to obtain the solutions of (1).

After these remarks we move onto the examples.

(a) \( 7x = 2 \) in \( \mathbb{Z}_{24} \) reduces to \( 7x - 24q = 2 \). Since \( \text{GCD}(7, 24) = 1 \) divides 2, we conclude that solutions exist. A particular solution is \( x_0 = 14 \), \( q_0 = 4 \) and thus all the solutions for \( x \) are \( x = 14 + 24t, \ t \in \mathbb{Z} \). As a result, the solutions of \( 7x = 2 \) in \( \mathbb{Z}_{24} \) are the classes \([14 + 24t]_{24}\) for \( t \in \mathbb{Z} \). Since, for every \( t \in \mathbb{Z}, \ [14 + 24t]_{24} = [14]_{24}, \) we conclude that \( 7x = 2 \) has the unique solution \([14]_{24}\) in \( \mathbb{Z}_{24} \). Of course, we usually drop the notation for equivalence class and say that the unique solution of \( 7x = 2 \) in \( \mathbb{Z}_{24} \) is \( x = 14 \).

(b) \( 34x = 14 \) in \( \mathbb{Z}_{51} \) reduces to \( 34x - 51q = 14 \). Since \( \text{GCD}(34, 51) = 17 \) does not divide 14, we conclude that there are no solutions.

(c) \( 15x = 5 \) in \( \mathbb{Z}_{65} \) reduces to \( 15x - 65q = 5 \). Since \( \text{GCD}(15, 65) = 5 \) divides 5, we conclude that solutions exist. A particular solution is \( x_0 = -4, q_0 = -1 \) and thus all the solutions for \( x \) are \( x = -4 + \frac{65}{5}t = -4 + 13t, \ t \in \mathbb{Z} \). As a result, the solutions of \( 15x = 5 \) in \( \mathbb{Z}_{65} \) are the classes \([−4+13t]_{65}\) for \( t \in \mathbb{Z} \). Since, for every \( t \in \mathbb{Z}, \ [−4+13t]_{65} \) equals one of the five distinct classes \([9]_{65}, [22]_{65}, [35]_{65}, [48]_{65}, [61]_{65}\), we conclude that \( 15x = 5 \) has the following 5 solutions in \( \mathbb{Z}_{65} \): \([9]_{65}, [22]_{65}, [35]_{65}, [48]_{65}, [61]_{65}\). Again, after dropping the notation for equivalence class, we say that the solutions of \( 15x = 5 \) in \( \mathbb{Z}_{65} \) are \( x = 9, 22, 35, 48, 61 \).

3. Let \( S \) denote the set of positive real numbers. Define operations \( \oplus \) and \( \odot \) by the equations

\[
x \oplus y := xy \quad \text{and} \quad x \odot y := x^{\ln y}.
\]

(a) Prove that \( S \) with the operations \( \oplus \) and \( \odot \) is a ring. What are \( 0_S \) and \( 1_S \)?

(b) Is \( S \) commutative?

(c) Find the units and the zero divisors in \( S \). For every unit \( u \in S \), find its inverse \( v \), i.e., \( v \in S \) such that \( u \odot v = v \odot u = 1_S \).

Solution. We need to verify that the operations \( \oplus \) and \( \odot \) in \( S \) satisfy the axioms of a ring. Please, make sure that you understand each of the arguments!

(i) \( (x \oplus y) \oplus z = (xy) \oplus z = (xy)z = x(yz) = x \oplus (yz) = x \oplus (y \oplus z); \)

(ii) \( x \oplus y = xy = y \oplus x; \)
(iii) the equation \( 1 \oplus x = 1x = x \) shows that 1 is the zero \( 0_S \) for \( \oplus \) in \( S \);

(iv) for \( x \in S \), we have \( x \oplus \frac{1}{x} = x\frac{1}{x} = 1 = 0_S \), which shows that every element of \( S \) has an opposite element, namely \( \frac{1}{x} \) is the opposite of \( x \);

(v) \( (x \odot y) \odot z = (x^{\ln y}) \odot z = x^{\ln y \ln z} = x^{\ln (y^{\ln z})} = x \odot (y^{\ln z}) = x \odot (y \odot z) \);

(vi) the equations \( e \odot x = e^{\ln x} = x \) and \( x \odot e = x^{\ln e} = x \) show that \( e \) is the identity \( 1_S \) for \( \odot \) in \( S \);

(viii) \( (x \oplus y) \odot z = (xy) \odot z = (xy)^{\ln z} = x^{\ln y} y^{\ln z} = (x \odot z)(y \odot z) = x \odot z \odot y \odot z \) and

\[ x \odot (y \oplus z) = x \odot (yz) = x^{\ln (yz)} = x^{\ln y + \ln z} = x^{\ln y} x^{\ln z} = x^{\ln y \oplus x^{\ln z}} = x \odot y \odot x \odot z. \]

Moreover,

(ix) \( x \odot y = x^{\ln y} = (e^{\ln x})^{\ln y} = e^{\ln x \ln y} = e^{\ln y \ln x} = (e^{\ln y})^{\ln x} = y^{\ln x} = y \odot x \) shows that \( S \) is commutative.

If \( u \neq 1 = 0_S \in S \), consider \( v := e^{\frac{1}{\ln u}} \). We have

\[ v \odot u = v^{\ln u} = (e^{\frac{1}{\ln u}})^{\ln u} = e^{\frac{1}{\ln u} \ln u} = e^1 = e = 1_S. \]

Since \( S \) is commutative, we also have \( u \odot v = v \odot u = 1_S \). This shows that every nonzero element of \( S \) is a unit and hence there are no zero divisors in \( S \). In fact, we have verified that \( S \) is a field.

Remark. One can verify that the map \( \varphi : S \to \mathbb{R} \) given by \( \varphi(x) = \ln x \) is an isomorphism between the fields \( S \) and \( \mathbb{R} \), the latter with the usual operations. In fact, this observation can give a shorter solution of the whole problem. \( \square \)