MATH10101, for supervision in week 11. Non-linear congruences — SOLUTIONS

Q25. Show that a non-negative integer is congruent, modulo 3 as well as modulo 9, to the sum of its (decimal) digits; for example, 2019 is congruent to $2+0+1+9$ modulo 9.

Hint. An integer written in digits as $a_n a_{n-1} \dots a_1 a_0$ is equal to $10^n a_n + 10^{n-1} a_{n-1} + \dots + 10 a_1 + a_0$; look at this modulo 9.

Q25 - solution. Since $10 \equiv 1 \bmod 9$, one observes that, modulo 9, $10^n a_n + 10^{n-1} a_{n-1} + \dots + 10 a_1 + a_0 \equiv 1^n a_n + \dots + 1 a_1 + a_0 = a_n + \dots + a_1 + a_0$, i.e., the sum of the digits.

Q26. (i) Show that a square (of an integer) is never congruent to 2 mod 3.

(ii) Show that a sum of two squares is never congruent to 3 mod 4.

(iii) Show that the distance between the origin $(0,0,0)$ and the point (x,y,z) with integer coordinates in the three-dimensional space cannot be equal to $\sqrt{799}$. Hint: work modulo 8. (Questions like this arise in 3D computer graphics.)

Q26 - solution. (i) Looking at possible residues of squares modulo 3, we note that 2 does not occur:

n	$n^2 \bmod 3$
0	$0^2 = 0$
1	$1^2 = 1$
2	$2^2 \equiv (-1)^2 = 1$

(ii) Now let us find possible residues of squares modulo 4:

n	$n^2 \bmod 4$
0	$0^2 = 0$
1	$1^2 = 1$
2	$2^2 = 4 \equiv 0$
3	$3^2 \equiv (-1)^2 = 1$

A square is congruent to either 0 or 1 mod 4, hence a sum of two squares, m^2+n^2, is congruent to either $0+0=0$, or $0+1=1$, or $1+1=2$ but never to 3.

(iii) Assume for contradiction that there are $x,y,z \in \mathbb{Z}$ such that the distance from $(0,0,0)$ to (x,y,z) is $\sqrt{799}$. Recall that by the 3D Pythagoras Theorem this distance is $\sqrt{x^2+y^2+z^2}$. Thus we have

$$x^2+y^2+z^2 = 799.$$

Modulo 8 this gives

$$x^2+y^2+z^2 \equiv 7 \mod 8.$$

Let us look at the possible remainders of squares mod 8:

$x \mod 8$	0	1	2	3	4	5	6	7
$x^2 \mod 8$	0	1	4	1	0	1	4	1

A square is congruent to 0, 1 or 4 mod 8. Hence a sum of three squares can be congruent to one of the following mod 8:

$$0+0+0 \equiv 0, \quad 0+0+1 \equiv 1, \quad 0+0+4 \equiv 4, \quad 0+1+1 \equiv 2, \quad 0+1+4 \equiv 5 \mod 8,$$
$$0+4+4 \equiv 0, \quad 1+1+1 \equiv 3, \quad 1+1+4 \equiv 6, \quad 1+4+4 \equiv 1, \quad 4+4+4 \equiv 4 \mod 8.$$

In no case can a sum of three squares be congruent to 7 mod 8 — contradiction, showing that our assumption that such integer x, y, z exist was false.

Q27. Recall the proof in the notes of the result that there do **not** exist integers x, y such that $15x^2 - 7y^2 = 1$. See also PJE, q.1 on p.225.

Use similar ideas to show that there are no integral solutions to the following. (*Hint* Choose a modulus m and look at the equation mod m. It often makes sense to choose m so that one of the terms in the equation vanishes mod m.)

(i) $5x^2 - 14y^2 = 1$,

(ii) $2x^3 + 27y^4 = 23$ (hint: look at this modulo 9),

(iii) $7x^5 + 3y^4 = 4$,

(⋆)(iv) $3x^4 + 5y^9 = 1$.

Q27 - solution. (i) Assume that the equation $5x^2 - 14y^2 = 1$ has an integer solution (x, y). Then, modulo 7, we have the congruence $5x^2 \equiv 1 \mod 7$. Noting that 3 is the inverse of $5 \bmod 7$, i.e. $3 \times 5 \equiv 1 \mod 7$, we get an equivalent congruence $x^2 \equiv 3 \mod 7$. All possible residues of squares mod 7 are given in the following table:

n	$n^2 \bmod 7$
0	0
1	1
2	4
3	2
4	$4^2 \equiv (-3)^2 = 3^2 \equiv 2$
5	$5^2 \equiv (-2)^2 = 2^2 = 4$
6	$6^2 \equiv (-1)^2 = 1^2 = 1$

From the table we can see that in all cases $x^2 \not\equiv 3 \mod 7$ since squares are congruent to 0, 1, 2 or 4 mod 7. This contradiction proves that there are no integer solutions.

Note that modulus 5 does not help in this question: $-14y^2 \equiv y^2 \equiv 1$ has solutions mod 5. This shows that a Diophantine equation may have solutions modulo m (i.e., solutions in $\mathbb{Z}_m$) for some m but no solutions in $\mathbb{Z}$.

(ii) Using the hint given, the Diophantine equation $2x^3 + 27y^4 = 23$ becomes $2x^3 \equiv 23 \equiv 5 \mod 9$. Noting that 5 is the inverse of 2 modulo 9, we multiply both sides by 5 to get $x^3 \equiv 25 \equiv 7 \mod 9$. But from the following table we see that this is impossible:

$x \mod 9$	0	1	2	3	4	5	6	7	8
$x^3 \mod 9$	0	1	8	0	1	8	0	1	8

The contradiction proves that the equation has no integer solutions.

(iii) Look at $7x^5 + 3y^4 = 4$ modulo 7 to see if there are solutions to $3y^4 \equiv 4 \mod 7$. Multiply both sides of the congruence by 5 which is an inverse of 3 modulo 7, obtaining an equivalent congruence $15y^4 \equiv 20 \mod 7$ which is the same as $y^4 \equiv 6 \mod 7$. But y^4 cannot be congruent to 6 mod 7 since $y^4 = (y^2)^2$ is a square, and squares can only be congruent to 0, 1, 2 or 4 modulo 7. This contradiction proves that there are no integer solutions.

(⋆)(iv) Consider the equation modulo 5. It then becomes the congruence $3x^4 \equiv 1 \mod 5$. Let us show that this congruence, hence the original equation, has no integer solutions. The following table shows that the possible remainders of x^4 when divided by 5 are 0 and 1:

$x \mod 5$	0	1	2	3	4
$x^4 \mod 5$	0	1	1	1	1

Indeed, $2^4 = 16 \equiv 1 \mod 5$, $3^4 \equiv (-2)^4 \equiv 2^4$ and $4^4 \equiv (-1)^4 \equiv 1 \mod 5$. Therefore, $3x^4$ can only leave remainder 0 or remainder 3 when divided by 5, and never remainder 1. This contradiction proves that integer solutions of the equation do not exist.

Q28. Find all the possible remainders left by $a^3 + a^2 + 1$ when divided by 5 where $a \in \mathbb{Z}$. Show that 5 does not divide $a^3 + a^2 + 1$ for any $a \in \mathbb{Z}$.

Q28 - solution. Let us find all possible remainders left by $a^3 + a^2 + 1$ where $a \in \mathbb{Z}$. By modular arithmetic, the remainder of $a^3 + a^2 + 1$ modulo 5 depends only on the remainder of a, hence it is enough to consider five cases. We do this in the following table:

$a \mod 5$	0	1	2	3	4
$a^2 \mod 5$	0	1	4	4	1
$a^3 \mod 5$	0	1	3	2	4
$a^3 + a^2 + 1 \mod 5$	1	3	3	2	1

The row for $a^2 \mod 5$ is obtained by squaring the entries in the row for $a \mod 5$ and taking the remainder modulo 5. The row for $a^3 \mod 5$ is obtained by cubing the entries in the row for $a \mod 5$ and taking the remainder modulo 5. The last row of the table is obtained by adding the rows for a^2 and for a^3, adding 1, and taking the remainder mod 5. For example, looking at the last column: if $a \equiv 4 \mod 5$, then $a^2 \equiv 4^2 \equiv (-1)^2 \equiv 1 \mod 5$, $a^3 \equiv (-1)^3 \equiv -1 \equiv 4 \mod 5$, so $a^3 + a^2 + 1 \equiv 1 + 4 + 1 \equiv 1 \mod 5$.

Since remainder 0 does not appear in the last row, we conclude that $a^3 + a^2 + 1$ never leaves remainder 0 when divided by 5. That is, $a^3 + a^2 + 1$ is not divisible by 5 for all $a \in \mathbb{Z}$.

Q29. (i) Write out the multiplication tables for $(\mathbb{Z}_6, +)$ and $(\mathbb{Z}_6, \times)$.

(⋆)(ii) Write out the multiplication table for $(\mathbb{Z}_9^*, \times)$ and list the inverses of each element.

Q29 - solution.

$(\mathbb{Z}_6, +)$

$+$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

$(\mathbb{Z}_6, \times)$

$\times$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

$(\mathbb{Z}_9^*, \times)$

$\times$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[1]_9$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[2]_9$	$[2]_9$	$[4]_9$	$[8]_9$	$[1]_9$	$[5]_9$	$[7]_9$
$[4]_9$	$[4]_9$	$[8]_9$	$[7]_9$	$[2]_9$	$[1]_9$	$[5]_9$
$[5]_9$	$[5]_9$	$[1]_9$	$[2]_9$	$[7]_9$	$[8]_9$	$[4]_9$
$[7]_9$	$[7]_9$	$[5]_9$	$[1]_9$	$[8]_9$	$[4]_9$	$[2]_9$
$[8]_9$	$[8]_9$	$[7]_9$	$[5]_9$	$[4]_9$	$[2]_9$	$[1]_9$

Note that we are told to write the multiplication table for $\mathbb{Z}_9^*$ not $\mathbb{Z}_9$. It is a mistake to include rows for $[0]_9$, $[3]_9$ or $[6]_9$ because these congruence classes are **not** elements of the set $\mathbb{Z}_9^*$.

So the inverses of elements of $\mathbb{Z}_9^*$ are as follows:

$$[1]_9^{-1} = [1]_9, \quad [2]_9^{-1} = [5]_9, \quad [4]_9^{-1} = [7]_9, \quad [5]_9^{-1} = [2]_9, \quad [7]_9^{-1} = [4]_9, \quad [8]_9^{-1} = [8]_9.$$

Q30. For each of the following relations on the set $\mathbb{N}_4$ indicate whether it is reflexive, symmetric or transitive. **Give your reasons.**

(i) $\mathcal{R}_1 = \{(2,2), (2,3), (2,4), (3,2), (3,3), (3,4)\}$ [*Answer*: Not reflexive, Not symmetric, Is transitive]

(ii) $\mathcal{R}_2 = \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}$, [*Answer*: Is an equivalence relation!]

(iii) $\mathcal{R}_3 = \{(2,4), (4,2)\}$, [*Answer*: Not reflexive, Is symmetric, Not transitive]

(iv) $\mathcal{R}_4 = \{(1,1), (1,3), (2,2), (3,4), (3,3), (4,3), (3,1), (4,4)\}$,

(v) $\mathcal{R}_5 = \{(1,1), (2,2), (3,3), (4,4)\}$,

(⋆)(vi) $\mathcal{R}_6 = \{(1,1), (1,3), (1,4), (2,1), (2,3), (2,4), (3,1), (3,4)\}$.

Q30 - solution.

	Reflexive	Symmetric	Transitive
(i)	No	No	Yes
(ii)	Yes	Yes	Yes
(iii)	No	Yes	No
(iv)	Yes	Yes	No
(v)	Yes	Yes	Yes
(vi)	No	No	No

Reasons:

i) **Not reflexive:** $(1,1) \notin \mathcal{R}_1$,
Not symmetric: $(2,4) \in \mathcal{R}_1$ but $(4,2) \notin \mathcal{R}_1$.
ii) **All** properties satisfied (by inspection).
iii) **Not reflexive:** $(1,1) \notin \mathcal{R}_3$,
Not transitive: $(2,4), (4,2) \in \mathcal{R}_3$ but $(2,2) \notin \mathcal{R}_3$.
iv) **Not transitive**: $(4,3), (3,1) \in \mathcal{R}_4$ but $(4,1) \notin \mathcal{R}_4$.
v) **All** properties satisfied (by inspection).
vi) **Not reflexive**: $(2,2) \notin \mathcal{R}_6$,
Not symmetric: $(1,4) \in \mathcal{R}_6$ but $(4,1) \notin \mathcal{R}_6$,
Not transitive: $(3,1), (1,3) \in \mathcal{R}_6$ but $(3,3) \notin \mathcal{R}_6$.

Q31. For each of the following relations on $\mathbb{N}$, list the ordered pairs that belong to the relation and check whether the relation is reflexive, symmetric or transitive:

$\mathcal{R} = \{(x,y) \colon 2x + y = 9\}$,

$\mathcal{S} = \{(x,y) \colon x + y < 7\}$,

$\mathcal{T} = \{(x,y) \colon x^2 + y^2 = 999999\}$ (*hint*: use **Q26**)

Q31 - solution. $\mathcal{R} = \{(1,7), (2,5), (3,3), (4,1)\}$.

$\mathcal{S} = \{(1,1), (1,2), (1,3), (1,4), (1,5), (2,1), (2,2), (2,3), (2,4), (3,1), (3,2), (3,3), (4,1), (4,2), (5,1)\}$.

$\mathcal{T} = \varnothing$: indeed, $999999 \equiv 3 \bmod 4$ hence by **Q26**(ii), 999999 cannot be a sum of two squares.

None of $\mathcal{R}, \mathcal{S}, \mathcal{T}$ **is reflexive:** a reflexive relation must contain pairs (a,a) for all $a \in \mathbb{N}$, but none of these relations contains the pair $(2019, 2019)$.

Relation $\mathcal{R}$ is **not symmetric** since it contains $(1,7)$ but not $(7,1)$. Relation $\mathcal{R}$ is **not transitive** since it contains $(4,1)$ and $(1,7)$ but does not contain $(4,7)$.

Relation $\mathcal{S}$ **is symmetric:** indeed, if $(x,y) \in \mathcal{S}$, then $x + y < 7$, then $y + x < 7$ meaning that $(y,x) \in \mathcal{S}$. Relation $\mathcal{S}$ is **not transitive** since it contains $(4,1)$ and $(1,4)$ but not $(4,4)$.

Relation $\mathcal{T}$ **is both symmetric and transitive**. Indeed, every proposition which starts with $\forall (a,b) \in \mathcal{T}$ is *automatically true* when $\mathcal{T}$ is the empty set.

Q32. The relation $\sim$ on the set $\mathbb{Z}$ is defined as follows: for $a, b \in \mathbb{Z}$, $a \sim b$ if and only if $5 \,|(9a^2 + b^2)$. Prove that $\sim$ is an equivalence relation.

Q32 - solution. We show that $\sim$ is **reflexive**, that is, $a \sim a$ for every $a \in \mathbb{Z}$. Indeed, by definition of $\sim$, the statement $a \sim a$ is equivalent to $5 \,|(9a^2 + a^2)$, same as $5 \,|\, 10a^2$. Since $10a^2 = 5 \times 2a^2$, the statement is true by definition of $|$ for all $a \in \mathbb{Z}$.

We show that $\sim$ is **symmetric**, that is, $a \sim b$ implies $b \sim a$. Assume that $a \sim b$, meaning that $9a^2 + b^2 = 5k$ for some integer k. Then $9b^2 + a^2 = 10(a^2 + b^2) - (9a^2 + b^2) = 5(2a^3 + 2b^2 - k)$ is also divisible by 5. This proves that $b \sim a$.

We show that $\sim$ is **transitive**, that is, $a \sim b$ and $b \sim c$ implies $a \sim c$. Assume $a \sim b$ and $b \sim c$, which translates as $9a^2 + b^2 = 5k$ and $9b^2 + c^2 = 5\ell$ for some $k, \ell \in \mathbb{Z}$. Adding these two equations together, we obtain $9a^2 + 10b^2 + c^2 = 5(k + \ell)$, which implies that $9a^2 + c^2 = 5(k + \ell - 2b^2)$ is divisible by 5, so that $a \sim c$. Transitivity is proved.

Alternatively one may observe that $5 \,|(9a^2 + b^2)$ is equivalent to $-a^2 + b^2 \equiv 0 \mod 5$, in other words $a^2 \equiv b^2 \mod 5$. This form of the relation $\sim$ allows one to argue using reflexivity, symmetry and transitivity of congruence.

Q33. Consider the function $f \colon \mathbb{Z} \to \mathbb{Z}_7$ defined by the rule $f(a) = [a]_7$.

($\star$)(i) Is f injective? Justify your answer.

(ii) Is f surjective? Justify your answer.

(iii) Let $X \subseteq \mathbb{Z}$ be such that $|X| = 8$. Prove that there exist $x, y \in X$ such that $x \neq y$ and $x \equiv y \mod 7$.

Hint: consider the restriction of the function f onto the set X. Apply the Pigeonhole Principle. Write your proof carefully.

(iv) (*more difficult*) Students on a maths course are divided into seven supervision groups. Prove that the lecturer can select one or more supervision groups so that the total number of students in the selected groups is divisible by 7.

Q33 - solution.

($\star$)(i) The function f is not injective. Indeed, $f(7) = [7]_7 = [0]_7 = f(0)$ but $7 \neq 0$ in $\mathbb{Z}$.

(ii) The function f is surjective because by definition of $\mathbb{Z}_7$, every element of $\mathbb{Z}_7$ is of the form $[a]_7$ for some $a \in \mathbb{Z}$. This means that every element of $\mathbb{Z}_7$ is of the form $f(a)$ for some $a \in \mathbb{Z}$.

(iii) The restriction of f onto X is a function whose domain is X, of cardinality 8, and whose codomain is $\mathbb{Z}_7$. It was shown in the lectures that $|\mathbb{Z}_7| = 7$, and $8 > 7$. Hence the Pigeonhole

Principle applies which says that f is not injective. By definition this means that there are elements $x, y \in X$ such that $x \neq y$ but $f(x) = f(y)$. Then $[x]_7 = [y]_7$ which is equivalent to $x \equiv y \mod 7$.

(iv) Let $g_1, g_2, \ldots, g_7$ be the number of students in supervision group 1, supervision group 2, ..., supervision group 7, respectively. Consider the following eight integers:

$$s_0 = 0, \quad s_1 = g_1, \quad s_2 = g_1 + g_2, \quad \ldots, \quad s_7 = g_1 + g_2 + \cdots + g_7.$$

That is, $s_k = \sum_{i=0}^{k} g_i$. By part (iii), two of these integers are congruent mod 7: say, $s_k \equiv s_\ell \mod 7$ where $0 \leq k < \ell \leq 7$. But then 7 divides $s_\ell - s_k = g_{k+1} + \cdots + g_\ell$, which means that the lecturer can select groups $k+1, \ldots, \ell$.