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

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 $10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10 a_1 + a_0$; look at this modulo 9.

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.)

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

($\star$)(iv) $3x^4 + 5y^9 = 1$.

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 $a \in \mathbb{Z}$.

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

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

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

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

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**)

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.

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.