MA10209 ALGEBRA 1A : EXERCISES 5

Hand in answers to (H) questions on Moodle by 6pm on Tue 3 Nov.
Homepage: `http://people.bath.ac.uk/masadk/ma209/`

(W) = Warmup, (H) = Homework, (A) = Additional

1 (W). Determine which of the following congruences have solutions and, if so, describe the complete set of solutions.

$$\text{(i)}\quad 5x \equiv 9 \pmod{12}, \qquad\qquad \text{(ii)}\quad 15x \equiv 6 \pmod{21}.$$

2 (H). Determine which of the following congruences have solutions and, if so, describe the complete set of solutions.

$$\text{(i)}\quad 140x \equiv 98 \pmod{84}, \qquad\qquad \text{(ii)}\quad 28x \equiv 124 \pmod{116}.$$

3 (W). Solve the following system of congruences.

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad 3x \equiv 5 \pmod 7.$$

4 (H). Solve the following systems of congruences.

(i) $x \equiv 1 \pmod 7$, $x \equiv 4 \pmod 9$, $x \equiv -2 \pmod 5$.

(ii) $4x \equiv 6 \pmod{13}$, $3x \equiv 2 \pmod 8$.

5 (W). For $m, n \in \mathbb{Z}^+$, recall that $m \mid z$ and $n \mid z \;\Leftrightarrow\; \operatorname{lcm}(m,n) \mid z$, for $z \in \mathbb{Z}$.
Setting $k = \operatorname{lcm}(m,n)$, deduce that the map $\pi\colon \mathbb{Z}_k \to \mathbb{Z}_m \times \mathbb{Z}_n\colon [x]_k \mapsto \big([x]_m, [x]_n\big)$ is well-defined and injective. Show that π is surjective if and only if m and n are coprime.

6 (H). Determine which of the following systems have solutions and, if so, describe the complete set of solutions. Proceed as in the coprime case, but be aware that at a certain point you may find an obstruction to the existence of solutions.

(i) $x \equiv 7 \pmod{15}$, $x \equiv 5 \pmod 9$,

(ii) $x \equiv 4 \pmod{15}$, $x \equiv 7 \pmod 9$.

7 (W). Show that no positive integer of the form $4m+3$ is the sum of two squares. [Hint: what are the squares mod 4?]

8 (H). Show that there are infinitely many positive integers which are not the sum of three squares. [Hint: what are the squares mod 8?] Investigate whether a simliar argument, working mod 16, could give a similar result about four squares.

9 (A). Let p be a prime and set $S = \{1, \ldots, p-1\}$.

(i) For $k \in S$, show that there is a unique $k' \in S$ such that $k \cdot k' \equiv 1 \pmod{p}$.

(ii) Show that $k = k'$ if and only if $k = 1$ or $k = p - 1$.

(iii) Deduce that $(p-1)! \equiv -1 \pmod{p}$.

(iv) Find an example that shows that this result may not hold if p is not prime.

ADK 27 Oct 2020