University of Birmingham
School of Mathematics

1AC Algebra and Combinatorics

Problem Sheet 2: Algebra part

You should carefully write out your solutions to all the questions below.
Ensure you have read and understood the Canvas assignment for the problem sheet for instructions about submitting solutions to SUM questions.

AQ1. Let $a, b, c \in \mathbb{Z}$.

(a) Suppose that a is coprime to b, and $a \mid bc$. Prove that $a \mid c$.

(b) Suppose that a is coprime to b, and that $a \mid c$ and $b \mid c$. Prove that $ab \mid c$.

(c) Suppose that a is coprime to c, and that b is coprime to c. Prove that ab is coprime to c.

You should use Bézout's lemma in your proofs, but you should **not** *use the Fundamental Theorem of Arithmetic.*

AQ2. (SUM) Find all solutions $x, y \in \mathbb{Z}$ to the following Diophantine equations.

(a) $x^3 = 4y^2 + 4y - 3$

(b) $x^2 - 3x = 9y^2 - 6y + 1$

AQ3. (a) Prove Lemma 3.6(b):

Lemma. *Let $n \in \mathbb{N}$ and $a, b, a', b' \in \mathbb{Z}$. Suppose that $a \equiv b \bmod n$ and $a' \equiv b' \bmod n$. Then $aa' \equiv bb' \bmod n$.*

(b) Find the remainder when $14^{43} - 12^{23}$ is divided by 13.

AQ4. (SUM) Determine whether each of the following statements is true and justify your answer.

(a) Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Suppose that $ab \equiv b^2 \bmod n$. Then $a \equiv b \bmod n$ or $b \equiv 0 \bmod n$.

(b) Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Suppose that there exists $z \in \mathbb{Z}$ such that $az \equiv 1 \bmod n$. Then a is coprime to n.

(c) Let $n \in \mathbb{N}$ with n odd. Then $8^{n-1} \equiv 1 \bmod n$.

When you are asked to justify your answer it means you have to prove it if it is true and give a counterexample if it is not true.