MAST20022 Group Theory and Linear Algebra

Assignment 1

Due: 4pm Friday August 16

- ▻ Submission is by file upload on the LMS. Scans or photos must be of good quality.
- ▻ **You must complete the plagiarism declaration on the LMS.**
- ▻ All answers should be fully justified.
- ▻ Soliciting answers to assignment questions from internet forums is strictly forbidden.

1. Prove the following: $\forall a, b \in \mathbb{N} \qquad a \mid b \iff \gcd(a, b) = a$

2. (a) Use the Euclidean Algorithm to calculate $\gcd(12378, -3054)$.
   (b) Use your calculations from (a) to find $x, y \in \mathbb{Z}$ such that
   $$\gcd(12378, -3054) = x12378 + y(-3054)$$

3. (a) Solve the following simultaneous equations in (i) $\mathbb{Z}/5\mathbb{Z}$ and (ii) $\mathbb{Z}/11\mathbb{Z}$.
   $$\begin{aligned} 2x + 3y &= 4 \\ 3x - 2y &= 1 \end{aligned}$$
   (b) Find all $x \in \mathbb{Z}/10\mathbb{Z}$ such that $x^3 + 3x^2 + 2x = 0$

4. (a) Show that $\mathbb{Q}(i) = \{a + bi \,|\, a, b, \in \mathbb{Q}\} \subset \mathbb{C}$ is a field (using the usual operations on $\mathbb{C}$). (Hint: You may use that $\mathbb{C}$ is a field.)
   (b) Show that the field $\mathbb{Q}(i)$ is *not* algebraically closed.

5. Ada sends Xav a message using the RSA cryptosystem. Xav's public key is:
   $$\begin{aligned} m &= 69 = 3 \times 23 \\ e &= 15 \end{aligned}$$
   The letters of the alphabet are encoded as $a = 2, b = 3, \ldots, z = 27$.
   (a) Find $d \in \mathbb{N}$ such that $ed \equiv 1 \pmod{44}$
   (b) Ada sends the (encrypted) message '11 28 11 30 54 43'
   Decrypt the message to obtain an English word.