MAST20022 Group Theory and Linear Algebra

Assignment 1

Due: 4pm Wednesday August 19, 2020

1. (a) Use the Euclidean Algorithm to calculate $\gcd(864371, 735577)$.
   (b) Find integers λ and μ such that $\gcd(864371, 735577) = 864371\lambda + 735577\mu$.

2. (a) Prove that if m is an integer then either $m^2 = 0 \bmod 4$ or $m^2 = 1 \bmod 4$.
   (b) Use (a) to show that if $a \in \mathbb{Z}$ and $a = 3 \bmod 4$ then there do not exist integers x and y such that
$$x^2 + y^2 = a.$$

3. (a) Write down the multiplication table for $\mathbb{Z}/8\mathbb{Z}$.
   (b) Find all possible factorizations of $x^2 + 4x + 3 = 0$ into linear factors
   (with coefficients in $\mathbb{Z}/8\mathbb{Z}$).

4. (a) Carefully state the Euclidean algorithm for $\mathbb{Z}$ as a theorem.
   (b) Prove the Euclidean algorithm for $\mathbb{Z}$.

5. Let $a, b \in \mathbb{Z}_{>0}$. Prove that there exists a unique $\ell \in \mathbb{Z}_{>0}$ such that $\ell\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

6. Let $a, b, \ell \in \mathbb{Z}_{>0}$. Let
$$a = p_1^{a_1} \cdots p_r^{a_r} \qquad \text{and} \qquad b = p_1^{b_1} \cdots p_r^{b_r}$$
   be the prime factorizations of a and b. Prove that the following are equivalent.
   (A) $\ell\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.
   (B) ℓ satisfies
      (1) ℓ is a multiple of a and ℓ is a multiple of b, and
      (2) If $m \in \mathbb{Z}_{>0}$ and m is a multiple of a and m is a multiple of b then m is a multiple of ℓ.
   (C) $\ell = p_1^{\max(a_1,b_1)} \cdots p_r^{\max(a_r,b_r)}$.

7. (a) Show that $\mathbb{Q}(i) = \{a + bi \mid a, b, \in \mathbb{Q}\} \subseteq \mathbb{C}$ is a field.
   (b) Show that the field $\mathbb{Q}(i)$ is *not* algebraically closed.

8. Ada sends Xav a message using the RSA cryptosystem.
   Xav's public key is: $m = 69$ and $e = 15$.
   The letters of the alphabet are encoded as $a = 2, b = 3, \ldots, z = 27$.
   Ada sends the (encrypted) message '11 28 11 30 54 43'.
   Decrypt the message to obtain an English word.
   In your solution, explain thoroughly and carefully how you execute the process of decryption.