Math 120B Rings and Fields: Homework 2

Hand in questions 1, 3, 6, 7, 9, 12 & 13 at discussion on Tuesday 16th October

1. The equation $x^3 - 2x^2 - 3x = 0$ in $\mathbb{Z}_{12}$ has *six* solutions. Find them, and find all possible factorizations of the polynomial in $\mathbb{Z}_{12}$ into monic linear factors of the form $x - a$.

2. Find all solutions to the following equations:

   (a) $3x = 2$ in the field $\mathbb{Z}_7$; in the field $\mathbb{Z}_{23}$.

   (b) $x^2 + 2x + 2 = 0$ in $\mathbb{Z}_6$

   (c) $x^2 + 2x + 4 = 0$ in $\mathbb{Z}_6$

3. Find the characteristic of each ring:

   (a) $2\mathbb{Z}$.

   (b) $\mathbb{Z}_3 \times 3\mathbb{Z}$.

   (c) $\mathbb{Z}_3 \times \mathbb{Z}_3$.

   (d) $\mathbb{Z}_6 \times \mathbb{Z}_{15}$.

4. Let R be a commutative ring with unity and with characteristic 3. Compute and simplify the expression $(a + b)^9$ for any $a, b \in R$.

5. Recall that $a \in R$ is *idempotent* if $a^2 = a$. Show that a division ring contains exactly two idempotents.

6. Let E be a subdomain of an integral domain D: thus E is itself an integral domain with respect to the same operations as that on D.

   (a) Prove that the characteristic of E is equal to that of D.

   (b) Prove that $1_E = 1_D$.

   (c) Prove that $\{n \cdot 1 : n \in \mathbb{Z}\}$ is a subdomain of D contained in every subdomain E.

7. Prove that the characteristic of an integral domain is either 0 or prime.
   (*Hint: consider* $(m \cdot 1)(n \cdot 1)$ *in* D *if the characteristic is* $mn\ldots$)

8. The integers $n = 7, 11$ and 17 all have primitive roots (the groups of units $\mathbb{Z}_7^\times, \mathbb{Z}_{11}^\times$ and $\mathbb{Z}_{17}^\times$ are all cyclic). Find a generator (primitive root) for each group.

9. Use Fermat's theorem to compute the remainder when 37^{49} is divided by 7.

10. Compute the remainder when $2^{2^{17}} + 1$ is divided by 19.

11. Use Euler's Theorem to compute 7^{1000} in $\mathbb{Z}_{24}$.

12. (a) Prove that if p is prime, then 1 and $p - 1$ are the only elements of $\mathbb{Z}_p$ that are their own inverses.

    (b) Prove that $n \in \mathbb{N}_{\geq 2}$ is prime if and only if $(n-1)! \equiv -1 \mod n$.

13. Describe the structure of the group $\mathbb{Z}_{20}^\times$ in the language of the Fundamental Theorem of Finitely Generated Abelian Groups: for a challenge, find an explicit isomorphism with your answer!