Chapter 3

Section 3.2

Question:

14. a) Let \( p \) be a prime. Use the fact that \( \mathbb{F}_p^\times \) is a group to prove that \( a^{p-1} \equiv 1 \) (modulo \( p \)) for every integer \( a \) not congruent to zero.

Answer:

a) \( \mathbb{F}_p^\times = \{ \overline{1}, \overline{2}, \ldots, \overline{p-1} \} \) for a prime \( p \). \( |\mathbb{F}_p^\times| = p - 1 \), thus the order of any element of \( \mathbb{F}_p^\times \) divides \( p - 1 \). Hence \( \overline{a}^{p-1} = \overline{1} \), which means that for all \( a \in \mathbb{Z} \) such that \( a \neq 0 \) modulo \( p \), we have \( a^{p-1} \equiv 1 \) (modulo \( p \)).

Question:

b) Prove Fermat’s Theorem: For every integer \( a \), \( a^p \equiv a \) (modulo \( p \)).

Answer:

b) From a) we have that \( a^{p-1} \equiv 1 \) (modulo \( p \)), for all \( a \in \mathbb{Z} \) such that \( a \neq 0 \) (modulo \( p \)). This means that there exists an integer \( q \) such that \( a^{p-1} - qp = 1 \Rightarrow a^p - aqp = a \Rightarrow a^p \equiv a \) (modulo \( p \)).

Next, assume that \( a \equiv 0 \) (modulo \( p \)), then \( a = qp \) for some integer \( q \). Hence, \( a^p = a^{p-1}qp \Rightarrow a^p \equiv 0 \) (modulo \( p \)) \( \Rightarrow a^p \equiv a \) (modulo \( p \)).

Question:

15. a) By pairing elements with their inverses, prove that the product of all nonzero elements of \( \mathbb{F}_p^\times \) is \(-1\).

Answer:

a) Let \( p = 2 \) then \( 1 = -1 \) and the statement is true. Let \( p \) be an odd prime then in \( \mathbb{F}_p^\times \) we have that \( (\overline{1})^1 = 1 \) and \( (\overline{p-1})^{-1} = \overline{p-1} \) since \( (\overline{p-1})^2 = \overline{p^2 - 2p + 1} = \overline{1} \). Thus there is an even number of residues left \( \overline{2}, \overline{3}, \ldots, \overline{p-2} \) that can be paired with their respective inverses to obtain that \( \overline{2} \cdot \overline{3} \cdots \overline{p-2} = \overline{1} \). Hence, \( \overline{1} \cdot \overline{2} \cdots \overline{p-2} \cdot \overline{p-1} = -\overline{1} \).

Question:

b) Let \( p \) be a prime integer. Prove Wilson’s Theorem: \( (p-1)! \equiv -1 \) (modulo \( p \)).

Answer:

b) From a) we have that \( (p-1)(p-2)\ldots(2)(1) \equiv -1 \) (modulo \( p \)). Thus, \( (p-1)! \equiv -1 \) (modulo \( p \)).
Chapter 10

Section 1

Question:

6. Let $\mathbb{Q}[\alpha, \beta]$ denote the smallest subring of $\mathbb{C}$ containing $\mathbb{Q}, \alpha = \sqrt{2},$ and $\beta = \sqrt{3},$ and let $\gamma = \alpha + \beta.$ Prove that $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma].$

Answer:

Let $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ be the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}, \sqrt{2}$ and $\sqrt{3},$ and $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\sqrt{2} + \sqrt{3}.$ First note that $\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}] \Rightarrow \mathbb{Q}[\sqrt{2} + \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}].$ Next, note that

$$\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$$

as well as $(\sqrt{2} + \sqrt{3})^3 = 9\sqrt{3} + 11\sqrt{2} \Rightarrow \frac{(\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{3} + \sqrt{2})}{2} = \sqrt{2}.$

Hence $\alpha = \frac{\gamma^3 - 9\gamma}{2} \in \mathbb{Q}[\gamma]$ and $\beta = \gamma - \alpha \in \mathbb{Q}[\gamma]$ so $\mathbb{Q}[\alpha, \beta] \subseteq \mathbb{Q}[\gamma].$

Question:

13. An element $x$ of a ring $R$ is called nilpotent if some power of $x$ is zero. Prove that if $x$ is nilpotent, then $1 + x$ is a unit in $R.$

Answer:

Let $x$ be a nilpotent element of $R,$ and let $n$ be the smallest positive integer for which $x^n = 0.$ If $x = 0,$ then clearly $1 + x = 1$ is a unit in $R.$ So assume $x \in R$ and $x \neq 0.$ Note that $1 = (1 - x^n) = (1 + x)(1 - x + x^2 - x^3 + \cdots + (-1)^{n-1} x^{n-1})$ since $R$ is a ring, $(1 - x + x^2 - x^3 + \cdots + (-1)^{n-1} x^{n-1}) \in R,$ hence $(1 + x)$ is a unit in $R.$
Chapter 12

Section 6.

Question:
4. Determine the number of isomorphism classes of abelian groups of order 400.

Answer:

400 = 2^4 \cdot 5^2, and the isomorphism classes are

\[ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \ ; \ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25} \]
\[ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \ ; \ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \]
\[ \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \ ; \ \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_{25} \]
\[ \mathbb{Z}_{16} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \ ; \ \mathbb{Z}_{16} \times \mathbb{Z}_{25} \]
\[ \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \ ; \ \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_{25} \]