UPSC Civil Services Main 2004 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *If p is a prime number of the form $4n+1$, n a natural number, then show that the congruence $x^2 \equiv -1 \mod p$ is solvable.*

Solution. Consider the multiplicative group G of non-zero residue classes modulo p. In this group $[1]$ and $[p-1]$ are the only two elements which are there own inverses as the equation $x^2 = [1]$ has exactly two solutions in the field $\mathbb{Z}/p\mathbb{Z}$. Since order of G is $\phi(p) = p-1 = 4n$, the remaining $4n-2$ elements form $2n-1$ pairs, in each pair each element is the inverse of the other. Thus

$$\prod_{1<r<p-1} [r] = [1]$$

as each one of the $2n-1$ pairs when multiplied would give us $[1]$. Consequently

$$\prod_{1\leq r\leq p-1} [r] = [p-1] \implies (p-1)! \equiv p-1 \equiv -1 \mod p$$

This is Wilson's theorem. Now

$$\begin{aligned}
(p-1)! &= \big(1\cdot 2\cdot\ldots\cdot \frac{p-1}{2}\big)\big(\frac{p+1}{2}\cdot\ldots\cdot(p-1)\big) \\
&= \big(1\cdot 2\cdot\ldots\cdot \frac{p-1}{2}\big)\big(p-\frac{p-1}{2}\big)\big(p-\frac{p-3}{2}\big)\ldots(p-1)) \\
&\equiv (-1)^{\frac{p-1}{2}}\big((\frac{p-1}{2})!\big)^2 \mod p
\end{aligned}$$

Since $p \equiv 1 \mod 4, (-1)^{\frac{p-1}{2}} = 1$ and we get

$$\big((\frac{p-1}{2})!\big)^2 \equiv (p-1)! \equiv -1 \mod p$$

showing that the congruence $x^2 \equiv -1 \mod p$ is solvable. ∎

Question 1(b) *Let G be a group and let $a, b \in G$. If $ab = ba$ and $(O(a), O(b)) = 1$ then show that $O(ab) = O(a)O(b)$.*

Solution. Let $O(a) = l, O(b) = m$ and $O(ab) = k$. Now $(ab)^{lm} = a^{lm}b^{lm}$ because $ab = ba$. But $a^{lm} = (a^l)^m = e, b^{lm} = (b^m)^l = e$ therefore $(ab)^{lm} = e$ and consequently k divides lm. Also $e = (ab)^k = a^k b^k \Rightarrow a^k = b^{-k} \Rightarrow a^{km} = b^{-km} = e \Rightarrow l \mid km$, but $(l, m) = 1$, therefore $l \mid k$. Considering $e = a^{kl} = b^{-kl}$, we get $m \mid k$. Since $(l, m) = 1$, we get $lm \mid k$. Hence $k = lm$ completing the proof. ∎

Question 2(a) *Verify that the set E of the four roots of $x^4 - 1 = 0$ forms a multiplicative group. Also prove that a transformation $T, T(n) = i^n$ is a homomorphism from I_+ (group of all integers with addition) onto E under multiplication.*

Solution. Clearly $E = \{e^{\frac{2\pi i}{4}}, e^{\frac{4\pi i}{4}}, e^{\frac{6\pi i}{4}}, e^{\frac{8\pi i}{4}}\} = \{e^{\frac{\pi i}{2}}, e^{\pi i}, e^{\frac{3\pi i}{2}}, e^{2\pi i}\} = \{1, -1, i, -i\}$. The following multiplication table shows that E is a multiplication group.

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

In fact

1. $\alpha, \beta \in E \Rightarrow \alpha\beta \in E$
2. 1 is the multiplicative identity of E.
3. Each element of E has an inverse in E.
4. The operation of multiplication is associative in E as it is so in $\mathbb{C} - \{0\}$.

Now $T(n) = i^n = i, -1, -i, 1$ according as $n = 1, 2, 3, 0 \mod 4$. Thus T is a mapping from I_+ to E and it is clearly onto (note that $T(0) = 1, T(1) = i, T(2) = -1, T(3) = -i$). Moreover T is a homomorphism is obvious as $T(m + n) = i^{m+n} = i^m i^n = T(m)T(n)$. ∎

Question 2(b) *Prove that if the cancellation law holds for a ring R then $a(\neq 0) \in R$ is not a zero divisor and conversely.*

Solution. Assume the cancellation law holds. If $a \neq 0$ and $ab = 0$ for some $b \in R$, then we get $ab = a0$ and since $a \neq 0$, the cancellation law gives us $b = 0$, showing that a is not a zero divisor. Conversely assume R has no zero divisors. Let $a \neq 0$ and $ax = ay \Rightarrow a(x - y) = 0$. This should imply $x - y = 0$ because otherwise a will be a zero divisor. Thus $ax = ay, a \neq 0 \Longrightarrow x = y$ i.e. cancellation law holds. This completes the proof. ∎

Question 2(c) *Show that the residue class ring $\mathbb{Z}/(m)$ is a field if m is a prime number.*

Solution. We first show that $\mathbb{Z}/(m)$ is a commutative ring for all $m \geq 1$.

1. Let $[a] = \{x \mid x \in \mathbb{Z}, x \equiv a \mod m\}, [b] \in \mathbb{Z}/(m)$, then $[a] + [b] = [a + b]$ as $x \equiv a \mod m, y \equiv b \mod m \Rightarrow x + y \equiv a + b \mod m$.

2. $[a] + [b] = [a + b] = [b + a] = [b] + [a]$ for every $[a], [b] \in \mathbb{Z}/(m)$.

3. $[a] + [0] = [a + 0] = [a]$ for every $[a] \in \mathbb{Z}/(m)$.

4. If $[a] \in \mathbb{Z}/(m)$ then $[-a] \in \mathbb{Z}/(m)$ and $[a] + [-a] = [a + (-a)] = [0]$, hence $[-a]$ is the additive inverse of $[a]$.

5. $[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = [a + b] + [c] = ([a] + [b]) + [c]$ showing the operation is additive.

6. For $[a], [b] \in \mathbb{Z}/(m)$, $[a][b] = [ab] = [b][a]$ as $x \equiv a \mod m, y \equiv b \mod m \Rightarrow xy \equiv ab \mod m$. This shows that $\mathbb{Z}/(m)$ is closed with respect to the operation of multiplication of residue classes modulo m. Moreover this operation is commutative.

7. Clearly $[a]([b][c]) = [a][bc] = [abc] = ([a][b])[c]$, so multiplication is associative.

8. $[a]([b] + [c]) = [a][b + c] = [a(b + c)] = [ab + ac] = [a][b] + [a][c]$ and $([a] + [b])[c] = [a][c] + [b][c]$.

9. $[a][1] = [1][a] = [a]$.

Thus $\mathbb{Z}/(m)$ is a commutative ring with identity. To show that it is a field, we have to show that every non-zero element is invertible.

Let $[a] \in \mathbb{Z}/(m), [a] \neq [0]$. This means that $a \not\equiv 0 \mod m$. Since m is a prime, it follow that $(a, m) = 1$, and therefore there exist integers b and c such that $ab + cm = 1$. Consequently $ab \equiv 1 \mod m$, or $[a][b] = [1]$ i.e. $[a]$ is invertible and $[b]$ is its inverse.

Hence $\mathbb{Z}/(m)$ is a field when m is a prime.

Note: $\mathbb{Z}/(m)$ is not even an integral domain when $m > 1$ and is not prime. $m = bc$ where $1 < b < m, 1 < c < m$ and therefore $[b], [c] \neq [0]$ but $[b][c] = [bc] = [0]$, showing that $\mathbb{Z}/(m)$ has zero divisors and is not an integral domain. ∎

Question 2(d) *Define an irreducible element and a prime element in an integral domain D with unit. Prove that every prime element in D is irreducible, but the converse of this is not in general true,*

Solution. Irreducible element. An element $a \neq 0$ which is not a unit in D is said to be an irreducible element if $a = bc$ implies that either b or c is a unit (consequently either b or c is an associate of a).

Prime. An element $a \neq 0$, a not a unit is is said to be a prime element if $a \mid bc \Rightarrow a \mid b$ or $a \mid c$.

Every prime is irreducible. Let a be a prime element in D. If possible let $a = bc$, we shall show that either b or c is a unit. Since $a \mid bc$ and a is a prime element, $a \mid b$ or $a \mid c$. If $a \mid b$ then there exists $x \in D$ such that $b = xa \Longrightarrow a = xac$. But D is an integral domain and therefore cancellation holds. Thus $a = xac \Rightarrow 1 = xc$ i.e. c is a unit. Similarly we can show that if $a \mid c$ then b is a unit. Thus a is an irreducible element i.e. it has no proper divisors.

Example where an irreducible need not be prime.

$$D = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

We define for $\alpha \in D$, $N(\alpha) = a^2 + 5b^2$ where $\alpha = a + b\sqrt{-5}$. Clearly for $\alpha, \beta \in D$, $N(\alpha\beta) = N(\alpha)N(\beta)$. Moreover $\alpha \in D$ is a unit if and only if $N(\alpha) = 1$. Thus D has only two units namely ± 1.

Now we show that 2 is irreducible but not a prime. If possible, let $2 = \alpha\beta$, then $N(2) = 4 = N(\alpha)N(\beta)$, showing that $N(\alpha) = 1, 2, 4 \Rightarrow N(\beta) = 4, 2, 1$. If $N(\alpha) = 1$, then α is a unit, and if $N(\alpha) = 4$, then β is a unit. If $\alpha = a + b\sqrt{-5}$, then $N(\alpha) = 2 \Rightarrow a + 5b^2 = 2$, which is not possible for $a, b \in \mathbb{Z}$. Hence 2 is irreducible.

However $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, i.e. $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ but 2 does not divide either $(1 + \sqrt{-5})$ or $(1 - \sqrt{-5})$, because $N(2) = 4, N(1 \pm \sqrt{-5}) = 6$ and $4 \nmid 6$. Hence 2 is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$.

∎