# Assignment 2 Solutions

Vedantam Srivatsav

## Problem 1

**Question 1.**

Prove that if $m_1$ and $m_2$ are coprime, then there exists an integer $x$ satisfying:

$$x \equiv a \pmod{m_1}, \quad x \equiv b \pmod{m_2}$$

and that this solution is unique modulo $m_1 m_2$.

**Solution.**

1. **Existence:** we have,

$$\begin{aligned} (x-a) &\equiv 0 \pmod{m_1} \\ (x-b) &\equiv 0 \pmod{m_2} \\ \Rightarrow x - a &= m_1 y_1 \\ x - b &= m_2 y_2 \end{aligned}$$

subtracting both the equations, we get

$$b - a = m_1 y_1 - m_2 y_2$$

Since $m_1$ and $m_2$ are coprime, they span $\mathbb{Z}$, which means $\exists$ $y_1$, $y_2$, which form the solution for the above equation, hence if we have $y_1$ and $y_2$, we have the value of x.

2. **Uniqueness:** let $x_1$ and $x_2$ be two different solutions for the given modulo equations. We have,

$$\begin{aligned} x_1 - x_2 &\equiv 0 \pmod{m_1} \\ x_1 - x_2 &\equiv 0 \pmod{m_2} \end{aligned}$$

Since $m_1$ and $m_2$ are co-prime, we can say that $x_1 - x_2$ is divisible by the product $m_1 m_2$, hence we can say,

$$\begin{aligned} x_1 - x_2 &\equiv 0 \pmod{m} \quad \text{where m} = m_1 m_2 \\ \Rightarrow x_1 &\equiv x_2 \pmod{m} \end{aligned}$$

Hence we can say that $x_1$ and $x_2$ are unique modulo $m_1 m_2$.

□

# Problem 2

**Question 2.**

Show that the ring $\mathbb{Z}/(m_1m_2)\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ if and only if $m_1$ and $m_2$ are coprime.

**Solution.** □

# Problem 3

**Question 3.**

Define a ring isomorphism between $\mathbb{Z}_{15}$ and $\mathbb{Z}_3 \times \mathbb{Z}_5$. Use it to find the solution to:

$$x \equiv 2 \pmod 3, \quad x \equiv 4 \pmod 5$$

**Solution.**

- consider the ring isomorphism $f : \mathbb{Z}_{15} \to \mathbb{Z}_3 \times \mathbb{Z}_5$, where f is defined as $f(n) = (n \pmod 3, n \pmod 5)$. now we need to find a value for n, such that $f(n) = (2, 4)$.
- from CRT we know that there exists an unique solution for n.
- for finding the unique solution, we need to find the multiplicative inverses of $3 \pmod 5$ and $5 \pmod 3$, which we get as $(2, 2)$.
- so the value of n is given by:

$$n \equiv 4 \cdot 3 \cdot 2 + 2 \cdot 5 \cdot 2 \equiv 14 \pmod{15}$$

- Hence $n \equiv 44 \pmod{15}$ is the solution for the given set of equations.

□

# Problem 4

**Question 4.**

Define a finite field. What is the order of a finite field?

**Solution.**

- A finite field is a Field whose set has only a finite number of elements.
- the order of a finite field F is given by $p^n$, where p is the **charecteristic** of the Field F, and n is a non-negative integer. Note that the charecteristic of a Finite field is always a prime number.

□

# Problem 5

**Question 5.**

Prove that every finite field has order $p^n$ for some prime $p$ and integer $n \geq 1$.

**Solution.**

1. **Show that** there exists an isomorphism between a subfield of F and $\mathbb{Z}_p$
   let $\phi(n) : \mathbb{Z} \to F$ be a homomorphism, where $\phi(n) = n \cdot 1$, clearly, $p\mathbb{Z} = \text{kernel}(\phi)$, and the image will be a subfield of F.
   by the **first Isomorphism theorem**, which states that $\mathbb{Z}/p\mathbb{Z} \cong K$, where K is the image subfield of the homomorphism.

2. F is an extension over the subfield K, and is a vector space with dimension given by $[F : K] = n$ (where n is some positive integer), therefore every element in F can be represented as a linear combination of n unique elements in F, so we have:

   $$x = a_1x_1 + ... + a_nx_n$$

   where $a_1, ..., a_n \in K$ are the scalar co-efficients from K and $x_1, ..., x_n \in F$ are the basis elements of the field F, since K has an order of p, and there are p choices for every co-efficient because K is isomorphic to $\mathbb{Z}_p$ , we can say that a total of $p \cdot p \cdot p...(n - times) = p^n$ arbitrary elements can be formed from the basis elements.

Hence proved that every finite field has order $p^n$ for some prime p and integer $n \geq 1$. □

# Problem 6

**Question 6.**

Is $\mathbb{Z}_6$ a field? Justify your answer.

**Solution.**

- A commutative ring R, whose every element is a unit is called a **Field**.
- $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, elements 0,2,3,4 donot have any multiplicative inverses, as their gcd with 6 is greater than 1. Since not every element is a unit, we can say that $\mathbb{Z}_6$ is not a Field.

□

# Problem 7

**Question 7.**

In $\mathbb{F}_5 = \mathbb{Z}_5$, list all nonzero elements and verify which elements are generators of the multiplicative group.

**Solution.**

- the multiplicative group of the field $\mathbb{Z}_5$ is given by $\mathbb{Z}_5^*$ where * implies it is the set of all units (does not include 0).
- so the multiplicative group is : $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$, now if we list out all the generated sets of each element, we get:

$$\begin{aligned}
\langle a \rangle &= \{1, a, a^2, ..., a^{n-1}\} \\
\langle 1 \rangle &= \{1\} \\
\langle 2 \rangle &= \{1, 2, 4, 3\} \\
\langle 3 \rangle &= \{1, 3, 4, 2\} \\
\langle 4 \rangle &= \{1, 4, 1, 1, 4, ....\}
\end{aligned}$$

- from the above sets , it is clear that the generators are 2, 3.
- note that the primitive roots modulo p will be the generators of the multiplicative group $\mathbb{Z}_p^*$.

□

# Problem 8

**Question 8.**

How many elements are there in the field $\mathbb{F}_{16}$? Is it isomorphic to $\mathbb{Z}_{16}$?

**Solution.**

The order of both the sets is 16, but $\mathbb{Z}_{16}$ is not a field, as it has zero divisors ($2 \cdot 8 \equiv 0 (\text{mod } 16)$), so they cannot be isomorphic. □

# Problem 9

**Question 9.**

Construct the field $\mathbb{F}_4$ as $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

**Solution.**

- the field $\mathbb{Z}_2[x]/(x^2+x+1)$ contains the remainders mod$(x^2+x+1)$, so the set becomes:

  $F = \{a + b\alpha : a, b \in \{0, 1\}\}$ (a, b belong to {0,1} because the coefficients are taken mod 2)
  $\alpha \equiv x(\text{mod } x^2 + x + 1)$

- so in total we get four possible elements, 0, 1, x, x+1.
- from trivial addition and multiplications, we can see that this set satisfies:
  1. addition group properties
  2. commutative ring properties
  3. every element has a multiplicative inverse(example: $x^{-1} = x + 1$ in this field).

Hence we can say that this Quotient ring satisfies all the properties of a finite field, so we constructed $\mathbb{F}_4$. □

# Problem 10

**Question 10.**

What is the multiplicative inverse of $x$ in $\mathbb{F}_4$ constructed above?

**Solution.** The inverse of $x$ in this Field is given by $x + 1$, we can verify this fact:

$$\begin{aligned} x \cdot (x + 1) &= x^2 + x \\ x^2 + x &\equiv -1(\text{mod } x^2 + x + 1) \\ -1 &\equiv 1(\text{mod } 2) \end{aligned}$$

Hence we can say that $x + 1$ is the multiplicative inverse of x in the field $\mathbb{F}_4$ □

# Problem 11

**Question 11.**

Explain why $\mathbb{F}_p$ is a field but $\mathbb{Z}_n$ is not a field for composite $n$.

**Solution.**

- If n is composite, then we can write $n = a \cdot b$, where a, b are non-zero integers and also less than n.
- but if that is possible then we get:

  $$a \cdot b \equiv 0(\text{mod n})$$

  but neither a nor b is 0, making a,b zero-divisors in $\mathbb{Z}_n$.
- since $\mathbb{Z}_n$ contains zero-divisors, hence it doesnot make a field.

□

# Problem 12

**Question 12.**

If a polynomial of degree 2 or 3 over a field has no root in that field, prove that it is irreducible.

**Solution.**

- let's assume a polynomial p of degree 2, and it does not have any root in that field. let it be reducible, then we get $p(x) = q(x) \cdot r(x)$, where q(x) and r(x) are irreducible polynomials of degree $\geq 1$, since p(x) is of degree 2, we have q(x) and r(x) degrees to be 1.
- if their degree is 1, that is they are linear in the field, then we get:

$$\begin{aligned} q(x) &= ax + b \\ \Rightarrow q(-b/a) &= 0 \end{aligned}$$

  since a,b also exist in the Field, and $a^{-1}$ also exists in the field if a exists, we have -b/a in the field.
- which means $p(-b/a) = 0$, but p doesnot have any roots, which means q(x) must be a constant, therefore we can say that polynomials of degree 2 ( same reasoning for 3 as 3 = 2+1), are irreducible if they donot have any root in that field.

□

# Problem 13

**Question 13.**

Define an integral domain. Give an example that is not a field.

**Solution.**

**Definition 1.** *A commutative ring R with unity is called an* ***integral domain*** *if it does not contain any zero-divisors.*

**example**: $\mathbb{Z}$ is an integral domain but not a field, it is a commutative ring, it contains 1, and it does not have any zero divisors, but it is not a field as it does not contain the multiplicative inverses of the elements of the ring. □

# Problem 14

**Question 14.**

Arrange the following structures in order of implication (from strongest to weakest): Euclidean Domain, PID, UFD, Integral Domain. Explain each implication briefly.

**Solution.** First let's go through their definitions:

**Definition 2.** *A ring $R$ is said to be an **Euclidian Domain**, if $\exists$ a function $\lambda$ from $R$ to the set $\{0,1,2,....\}$ such that if $a, b \in R$ and $b \neq 0$, then $\exists\ c, d \in R$ with a property $a = bc + d$, and $0 \leq \lambda(d) < b$.*

**Definition 3.** *$R$ is said to be a **Principle Ideal Domain** if every ideal of $R$ is a principle ideal.*

**Definition 4.** *A ring $D$ is said to be UFD, if every element of $D$ can be written as a product of irreducible elements in $D$.*

**the final order of these domains is given by:** $ED < PID < UFD < ID$.

□

# Problem 15

**Question 15.**

Give an example of a UFD that is not a PID.

**Solution.** The ring $\mathbb{Z}[x]$ is a UFD but not a PID. □

# Problem 16

**Question 16.**

Is every PID a UFD? Is every UFD a PID? Justify with reasoning.

**Solution.** **YES**, every PID is an UFD, we can justify this using the finite ascending chain reasoning. But, every UFD **need not** be a PID, as we can see from the above example, $\mathbb{Z}[x]$ is a UFD, but not a PID. □

# Problem 17

**Question 17.**

Prove that $\mathbb{Z}[x]$ is a UFD but not a PID.

**Solution.**

- Consider the ideal $(2, x)$, assume it is both UFD and PID, which means the ideal $(2, x)$ should be represented as a principle ideal $\langle f(x) \rangle$.
- but that means $f(x)$ divides both of the generators of the ideal, that is 2 and x.

- which means it also divides the gcd(2,x), giving us $f(x) = \pm 1$, but that makes it a unit. which means $\langle f(x) \rangle = \mathbb{Z}[x]$, but (2,x) is clearly not the whole ring.
- We also know that if D is a UFD, then $D[x]$ is also a UFD.
- hence $\mathbb{Z}[x]$ is a UFD, but not a PID.

□

# Problem 18

**Question 18.**

State and explain the First Isomorphism Theorem in your own words.

**Solution.**

**Theorem 1.** ***The first isomorphism theorem*** *states that for every Homomorphism $\phi : G \to H$ the Quotient group of the kernel($\phi$) is isomorphic to the image of $\phi$. That is:*

$$G/ker(\phi) \cong im(\phi)$$

□

# Problem 19

**Question 19.**

Let $\varphi : \mathbb{Z} \to \mathbb{Z}_5$, $\varphi(n) = n \bmod 5$. Use the First Isomorphism Theorem to describe $\mathbb{Z}/\ker\varphi$.

**Solution.** From the first isomorphism theorem, we can say that:

$$\mathbb{Z}/ker(\varphi) \cong img(\varphi)$$

the image of this homomorphism is equal to $\mathbb{Z}_5$, hence we can say that,

$$\mathbb{Z}/ker(\varphi) \cong \mathbb{Z}_5$$

□

# Problem 20

**Question 20.**

Let $G = \mathbb{Z}_{12}^*$. List all elements and find the order of each.

**Solution.** $G = \mathbb{Z}_{12}^*$ is the set of all units in $\mathbb{Z}_{12}$.

$$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$$

1. order of 1 is 1
2. order of 5 is 2
3. order of 7 is 2
4. order of 11 is 2

□

# Problem 21

**Question 21.**

Suppose $H$ is a subgroup of $G$ and $|G| = 18$, what are the possible orders of $H$? List them and explain why.

**Solution.**
By **lagrange's theorem**, the order of the subgroup should divide the order of the group. Hence we get the possible orders of H to be : {1,2,3,6,9,18}. □

# Problem 22

**Question 22.**

Define the Dirichlet convolution $(f * g)(n)$. Suppose $f(n) = \varphi(n)$. Show that:

$$\sum_{d|n} \varphi(d) = n$$

Use Möbius inversion to recover $\varphi(n)$ from this identity.

**Solution.**

1. **Dirichlet convolution** between two function f and g is defined as:

$$(f * g)(n) = \Sigma f(d_1) \cdot g(d_2)$$

where the sum is over all the pairs $(d_1, d_2)$ such that $d_1 \cdot d_2 = n$.

2. consider the fractions:
$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, ...., \frac{n}{n}$$
if b is a divisor of n, exactly $\phi(b)$ elements will reduce to the form $\frac{a}{b}$, where $gcd(a, b) = 1$ and $a < b$. Since the total number of fractions is n, we can say that,
$$\sum_{d|n} \varphi(d) = n$$

3. using mobius inversion on the second result, we can say that,
$$\sum_{d|n} \varphi(d) = n \Rightarrow \sum_{d|n} n/d \cdot \mu(d) = \varphi(n)$$
we get $\varphi(n)$ using this identity.

□

# Problem 23

**Question 23.**

Let $f(n) = \sum_{d|n} \mu(d) \log d$. Is $f(n)$ always zero? Justify your answer.

**Solution.**

□

# Problem 24 Bonus

**Question 24.**

Let $F = \mathbb{F}_2[x]/(x^2 + x + 1)$. Show that every non-zero element in $F$ has a multiplicative inverse. **Solution.** □

**Question 25.**

Prove that the multiplicative group of any finite field is cyclic. **Solution.** □

**Question 26.**

Find a polynomial $f(x) \in \mathbb{F}_2[x]$ of degree 4 which is irreducible. **Solution.** □