Problem Set 3 Solutions

Igor Rapinchuk

1. (a) $3x \equiv 7(\text{modulo } 25)$. Since $3(-8) = -24 \equiv 1(\text{modulo } 25)$, we have $3^{-1} \equiv -8(\text{modulo } 25)$. Then $x = (-8) \cdot 7 = -56 \equiv -6(\text{modulo } 25)$. Check: $3(-6) = -18 \equiv 7(\text{modulo } 25)$.

(b) $3x \equiv 7(\text{modulo } 15)$. This equation has no solutions. Indeed, this congruence is equivalent to $3x = 7 + 15y$ for some $y \in \mathbb{Z}$. Then $7 = 15y - 3x$. But the right-hand side is divisible by 3, while the left-hand side is not. A contradiction.

2. Let z be a positive integer. Then $z = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$, where $a_i \in \{0, 1, 2, \ldots, 9\}$. We have $10 \equiv 1 \pmod 9$ and we prove by induction that $10^n \equiv 1 \pmod 9$ for $n \in \mathbb{Z}_{\geqslant 0}$. Then

$$z = \sum_{i=1}^{k}(a_k \cdot 10^k + \cdots + a_0) \equiv \sum_{i=1}^{k}(a_k + \cdots + a_0) \pmod 9.$$

Now let z be as above. We have $10 \equiv -1 \pmod{11}$ and we prove by induction that $10^n \equiv (-1)^n \pmod{11}$ for $n \in \mathbb{Z}_{\geqslant 0}$. So,

$$z = \sum_{i=1}^{k}(a_k \cdot 10^k + \cdots + a_0) \equiv \sum_{i=1}^{k}((-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots - a_1 + a_0) \pmod{11}.$$

3. Since the g.c.d. of m and n is 1, by Proposition 2.2.6 there exist integers r and s such that $mr + ns = 1$. Set $c = mr$ and $d = ns$. Then

$$c \equiv 0(\text{modulo } m) \quad , \quad c \equiv 1(\text{modulo } n)$$

and

$$d \equiv 1(\text{modulo } m) \quad , \quad d \equiv 0(\text{modulo } n)$$

Let $x = bc + ad$. Then

$$x \equiv b \cdot 0 + a \cdot 1 = a(\text{modulo } m)$$

and

$$x \equiv b \cdot 1 + a \cdot 0 = b(\text{modulo } n)$$

So, x is a required element.

4. Direct computation shows that $(eH)((123)H) = (eH)((132)H) = \{(123), (13), (23), (132)\}$. This set is not a coset of H because every coset contains two elements.

5. First, let us show that N is a subgroup of G. For this, we need to show that N is closed under multiplication and under taking inverses. To show that N is closed under multiplication, observe that $NN \subset N$ as we have $e \cdot e = e \in N$. Next, let $g \in N$. Then, we claim that $g^{-1} \in N$. Suppose that $g^{-1} \in C$, for some $C \in P$. Then, since $e \in NC$ and $C \subset NC$, we have that $g^{-1} \in C \subset NC \subset N$. So, N is a subgroup.

Now let us show that P is the set of cosets of N. Take $A \in P$ and let $a \in A$. Then $aN = A$. Since $AN \subset A$, we have that $aN \subset A$. Now let $C \in P$ be the element of the partition that contains a^{-1}. Then, $Ca \subset N \Rightarrow a^{-1}A \subset N \Rightarrow A \subset aN$. So, $A = aN$.

Finally, let us show that N is a normal subgroup. For this, we need to show that $gNg^{-1} = N$ for all $g \in G$. If $g \in N$, then there is nothing to prove. So suppose $g \notin N$. Let $C \in P$ such that $g \in C$. Then $gN \subset C$ as $g \cdot e = g \in gN$. So $gNg^{-1} \subset Cg^{-1}$. But, because $e \in Cg^{-1}$, we have $Cg^{-1} \subset N$, so that $gNg^{-1} \subset N$. Since this is true for all $g \in G$, we may use g^{-1} instead of g, obtaining $g^{-1}N(g^{-1})^{-1} = g^{-1}Ng \subset N \Rightarrow N \subset gNg^{-1}$. So, $N = gNg^{-1}$, which shows that N is a normal subgroup.

6. For $(g, 1) \in G \times 1$, $(h, 1) \in G \times 1$, we have

$$(g, 1)(h, 1) = (gh, 1) \in G \times 1 \quad \text{and} \quad (g, 1)^{-1} = (g^{-1}, 1) \in G \times 1$$

For $(g, 1) \in G \times 1$ and $(a, b) \in G \times G'$ we have

$$(a, b)(g, 1)(a, b)^{-1} = (a, b)(g, 1)(a^{-1}, b^{-1}) = (aga^{-1}, 1) \in G \times 1$$

So, $G \times 1$ is a normal subgroup. Now, consider the map $\alpha\colon G \to G \times 1$ given by: $\alpha(g) = (g, 1)$. Clearly, α is a bijective map. It is also a group homomorphism:

$$\alpha(xy) = (xy, 1) = (x, 1)(y, 1) = \alpha(x)\alpha(y)$$

for all $x, y \in G$. So, α is a group isomorphism between G and $G \times 1$, and therefore these groups are isomorphic.

Consider the projection $\varphi\colon G \times G' \to G'$, $\varphi(g, g') = g'$. Then φ is a group homomorphism because

$$\varphi((g_1, g_1')(g_2, g_2')) = \varphi(g_1g_2, g_1'g_2') = g_1'g_2'$$

and

$$\varphi(g_1, g_1')\varphi(g_2, g_2') = g_1'g_2'$$

Clearly, $G \times 1 = \ker \varphi$, which, in particular, also implies that $G \times 1$ is a normal subgroup of $G \times G'$. The homomorphism φ is surjective. So, by the First Isomorphism Theorem

$$(G \times G')/(G \times 1) \approx G'$$

This isomorphism can be described explicitly as follows

$$(g, g')(G \times 1) \to g'$$

7. By the First Isomorphism Theorem, to prove that G/H is isomorphic to G, we need to construct a surjective group homomorphism $\varphi\colon G \to G$ with kernel H. Since H consists of all fourth roots of unity, it makes sense to try the map $\varphi(z) = z^4$. This map is a homomorphism because

$$\varphi(z_1z_2) = (z_1z_2)^4 = z_1^4z_2^4 = \varphi(z_1)\varphi(z_2)$$

This homomorphism is surjective. Indeed, any nonzero complex number z can be written in the trigonometric form,

$$z = r(\cos\theta + i\sin\theta), \quad r > 0$$

Then for

$$w = \sqrt[4]{r}(\cos(\theta/4) + i\sin(\theta/4))$$

one has $w^4 = z$, so $\varphi(w) = z$. The kernel of φ consists of those z for which $\varphi(z) = z^4 = 1$. It follows that $\ker\varphi$ consists of all fourth roots of unity, and therefor $\ker\varphi = H$. The coset aH can be characterized as the fiber of φ over $\varphi(a)$. So,

$$aH = \{z \in G \mid z^4 = a^4\}.$$

8. Consider the map $\varphi\colon \mathbb{R} \to U$ given by

$$\varphi(x) = e^{2\pi i x} = \cos(2\pi x) + i\sin(2\pi x) \in U$$

This map is a group homomorphism because

$$\varphi(x)\varphi(y) = (\cos(2\pi x) + i\sin(2\pi x))(\cos(2\pi x) + i\sin(2\pi x)) =$$

$$(\cos(2\pi x)\cos(2\pi y) - \sin(2\pi x)\sin(2\pi y)) + i(\sin(2\pi x)\cos(2\pi y) + \cos(2\pi x)\sin(2\pi y))$$

$$= \cos(2\pi(x+y)) + i\sin(2\pi(x+y)) = \varphi(x+y)$$

for all $x, y \in \mathbb{R}$. This homomorphism is surjective because any complex number z with $\mid z \mid = 1$ is of the form $\cos\alpha + \imath\sin\alpha$. The kernel of φ consists of $x \in \mathbb{R}$ for which

$$\cos(2\pi x) + i\sin(2\pi x) = 1 = \cos 0 + i\sin 0$$

Then $2\pi x = 2\pi k$, $k \in \mathbb{Z}$, so $x = k \in \mathbb{Z}$. So, $\ker\varphi = \mathbb{Z}$. By the First Isomorphism Theorem, $\mathbb{R}/\mathbb{Z} \approx U$. Explicitly, this isomorphism is given by

$$x + \mathbb{Z} \to \cos(2\pi x) + i\sin(2\pi x)$$

9. Let V be the vector space of all real $n \times n$ matrices.

(a) $W_1 = \{A \in V \mid A = {}^tA\}$ is a subspace of V because it is closed under addition and scalar multiplication. Indeed, suppose $A, B \in W_1$. Then ${}^tA = A$ and ${}^tB = B$. It follows that

$${}^t(A+B) = {}^tA + {}^tB = A + B,$$

so $A + B \in W_1$. For any $A \in W_1$ and any $c \in \mathbb{R}$, we have

$${}^t(cA) = c{}^tA = cA,$$

so $cA \in W_1$.

(b) $W_2 =$ subset of invertible matrices, is not a subspace because it is not closed under scalar multiplication. Namely, the identity matrix I_n belongs to W_2, but $0 \cdot I_n = O$ (zero matrix) does not.

(c) $W_3 =$ subset of upper triangular matrices. It is a subspace because it is closed under addition and scalar multiplication. To prove this, we observe $A = (a_{ij})$ belongs to W_3 iff $a_{ij} = 0$ for all $i > j$. If $A, B \in W_3$ then for any $i > j$ we have

$$(A+B)_{ij} = a_{ij} + b_{ij} = 0,$$

so $A + B \in W_3$. If $A \in W_3$ and $c \in \mathbb{R}$, we have

$$(cA)_{ij} = ca_{ij} = 0 \quad \text{for} \quad i > j,$$

so $cA \in W_3$.

10. (a) $p = 5$. $\det A = 42 \equiv 2 (\text{modulo } 5)$. Since $2^{-1} \equiv 3 (\text{modulo } 5)$, we have

$$A^{-1} = 3\begin{bmatrix} 6 & -3 \\ -2 & 8 \end{bmatrix} = \begin{bmatrix} 18 & -9 \\ -6 & 24 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 4 & 4 \end{bmatrix}$$

Check:

$$AA^{-1} = \begin{bmatrix} 8 & 3 \\ 2 & 6 \end{bmatrix}\begin{bmatrix} 3 & 1 \\ 4 & 4 \end{bmatrix} = \begin{bmatrix} 36 & 20 \\ 30 & 26 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

So,

$$X = A^{-1}B = \begin{bmatrix} 3 & 1 \\ 4 & 4 \end{bmatrix} = \begin{bmatrix} 3 \\ -1 \end{bmatrix} = \begin{bmatrix} 8 \\ 8 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \end{bmatrix}$$

Check:

$$\begin{bmatrix} 8 & 3 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} 3 \\ 3 \end{bmatrix} = \begin{bmatrix} 33 \\ 24 \end{bmatrix} = \begin{bmatrix} 3 \\ -1 \end{bmatrix}$$

$p = 17$. $\det A = 42 = 8(\text{modulo } 17)$. Since $8^{-1} \equiv -2(\text{modulo } 17)$, we have

$$A^{-1} = (-2) \begin{bmatrix} 6 & -3 \\ -2 & 8 \end{bmatrix} = \begin{bmatrix} -12 & 6 \\ 4 & -16 \end{bmatrix} = \begin{bmatrix} 5 & 6 \\ 4 & 1 \end{bmatrix}$$

Check:

$$AA^{-1} = \begin{bmatrix} 8 & 3 \\ 2 & 6 \end{bmatrix} = \begin{bmatrix} 5 & 6 \\ 4 & 1 \end{bmatrix} = \begin{bmatrix} 52 & 51 \\ 34 & 18 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

So,

$$X = A^{-1}B = \begin{bmatrix} 5 & 6 \\ 4 & 1 \end{bmatrix} = \begin{bmatrix} 3 \\ -1 \end{bmatrix} = \begin{bmatrix} 9 \\ 11 \end{bmatrix}$$

Check:

$$\begin{bmatrix} 8 & 3 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} 9 \\ 11 \end{bmatrix} = \begin{bmatrix} 105 \\ 84 \end{bmatrix} = \begin{bmatrix} 3 \\ -1 \end{bmatrix}$$

(b) $p = 7$. $\det A = 42 \equiv 0(\text{modulo } 7)$, so A^{-1} does not exist. Let us reduce the augmented matrix $[A \mid B]$.

$$\left[\begin{array}{cc|c} 8 & 3 & 3 \\ 2 & 6 & -1 \end{array}\right] = \left[\begin{array}{cc|c} 1 & 3 & 3 \\ 2 & 6 & -1 \end{array}\right] \rightarrow \left[\begin{array}{cc|c} 1 & 3 & 3 \\ 0 & 0 & -7 \end{array}\right] = \left[\begin{array}{cc|c} 1 & 3 & 3 \\ 0 & 0 & 0 \end{array}\right]$$

So, the system is equivalent to the single equation $x_1 + 3x_2 = 3 \Rightarrow x_1 = 3 - 3x_2$. So, the solution set is

$$\{(3 - 3x_2, x_2) \mid x_2 \in \mathbb{F}_7\}$$

It follows that the system has 7 solutions.