Exam 1 solutions

Math 116: Finashin, Pamuk, Pierce, Solak

Thursday, April 7, 2011

Problem 1. *(15 pts)*

(a) Find the greatest common divisor d of 453 and 213. Present d in the form $d = 453x + 213y$.

(b) If there is one, find a solution to $213x \equiv 12 \pmod{453}$.

(c) Find the least positive integer in $\{4530x + 2139y \colon x, y \in \mathbb{Z}\}$.

Solution. (a) First apply the Euclidean algorithm:

$$\begin{aligned}
453 &= 213 \cdot 2 + 27, \\
213 &= 27 \cdot 7 + 24, \\
27 &= 24 \cdot 1 + 3, \\
24 &= 3 \cdot 8.
\end{aligned}$$

So $\gcd(453, 213) = 3$. Also we compute

$$\begin{aligned}
3 &= 27 - 24 \\
&= 27 - (213 - 27 \cdot 7) \\
&= 27 \cdot 8 - 213 \\
&= (453 - 213 \cdot 2) \cdot 8 - 213 \\
&= 453 \cdot 8 - 213 \cdot 17.
\end{aligned}$$

(b) By (a), we have $3 \equiv 213 \cdot -17 \pmod{453}$, so

$$213x \equiv 12 \iff 213x \equiv 4 \cdot 3 \equiv 213 \cdot -68.$$

Therefore the congruence is solved when $x \equiv -68 \equiv 385 \pmod{453}$.

(c) $4530x + 2130y = 10(453x + 213y)$, so the least positive integer in the given set is $10 \cdot 3$, or $\boxed{30}$.

Remark. 1. There is a reason why the three parts of this problem are together. One application of the Euclidean algorithm is enough to give the answers of all three parts. (Some people used the algorithm two or three times; this was unnecessary.)

2. The second half of part (a) does not ask you to write "$3 = 453x+213y$" and then stop; it asks for a solution to this equation.

3. In part (b), one may observe that 3 divides each of 213, 12, and 453, so that

$$213x \equiv 12 \pmod{453} \iff 71x \equiv 4 \pmod{151}.$$

From part (a) we have $1 = 151 \cdot 8 + 71 \cdot -17$, so the congruence is solved by

$$\begin{aligned} x &\equiv 4 \cdot -17 \equiv -68 \equiv 83 \pmod{151}, \\ x &\equiv 83, 234, 385 \pmod{453}. \end{aligned}$$

This is the complete solution, but it was not required to find this: the problem asked just for *one* solution.

4. In part (c), some people seemed to confuse the *least* positive integer in the given set with the *least* common multiple of 4530 and 2130.

5. Part (c) does not ask for the values of x and y such that $4530x + 2130y$ is minimized among positive integers; it asks for the minimum possible positive value of this expression.

Problem 2. *(8pts) Let G be the set of even integers and $*$ be the binary operation on G defined by $x * y = x + y + 4$. Determine whether $(G, *)$ is a group or not. Prove your claim.*

Solution. Since x, y, are 4 are even, their sum is also even; so G is closed under $*$. To simplify some computations, we may note also that, since $+$ is commutative, so is $*$. Let us check for an identity. We claim that -4 is an identity with respect to $*$. Indeed,

$$x * (-4) = x - 4 + 4 = x$$

(and therefore also $(-4) * x = x$, by commutativity of $*$). So -4 is an identity. Considering

$$\begin{aligned} x * (y * z) &= x * (y + z + 4) \\ &= x + (y + z + 4) + 4 \\ &= (x + y + 4) + z + 4 \\ &= (x + y + 4) * z \\ &= (x * y) * z, \end{aligned}$$

we have that $*$ is associative. Now check for inverses. We claim that $-x - 8$ is the inverse of x with respect to $*$. We have

$$x * (-x - 8) = x - x - 8 + 4 = -4$$

(hence also $(-x - 8) * x = -4$). Therefore $(G, *)$ is a group.

Problem 3. *(7pts) Let $a * b = a + b + 3ab$, does $*$ define a binary operation on the set $\mathbb{Q}_+$ of positive rationals ? Is $*$ associative? Explain.*

Solution. Since the sum and product of two positive rationals is again a positive rational, $\mathbb{Q}_+$ is closed under $*$. Therefore $*$ is a binary operation on $\mathbb{Q}_+$.

For the associativity, we have

$$\begin{aligned} a * (b * c) &= a * (b + c + 3bc) \\ &= a + (b + c + 3bc) + 3a(b + c + 3bc) \\ &= a + b + c + 3bc + 3ab + 3ac + 9abc. \end{aligned}$$

while

$$\begin{aligned} (a * b) * c &= (a + b + 3ab) * c \\ &= (a + b + 3ab) + c + 3(a + b + 3ab)c \\ &= a + b + 3ab + c + 3ac + 3bc + 9abc. \end{aligned}$$

So we see that $a * (b * c) = (a * b) * c$. Hence $*$ is an associative binary operation on $\mathbb{Q}_+$.

Problem 4. *(15pts) Let G be the group $(\mathbb{Z}_{28}, +)$.*

(a) Find all generators of G.

(b) List all the subgroups of G. For each subgroup, different from G, write down all its elements.

Solution. (a) When $0 \leq k < 28$, we have $k = 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27$ if and only if $\gcd(k, 28) = 1$. Therefore the generators of G are [1], [3], [5], [9], [11], [13], [15], [17], [19], [23], [25], [27].

(b) The subgroups of G are $\langle [d] \rangle$, where $d \mid 28$; so they are

$$\langle [1] \rangle, \qquad \langle [2] \rangle, \qquad \langle [4] \rangle, \qquad \langle [7] \rangle, \qquad \langle [14] \rangle, \qquad \langle [28] \rangle.$$

Moreover,

$$\begin{aligned} \langle [1] \rangle &= \mathbb{Z}_{28} \\ \langle [2] \rangle &= \{[2], [4], [6], [8], [10], [12], [14], [16], [18], [20], [22], [24], [26], [0]\} \\ \langle [4] \rangle &= \{[4], [8], [12], [16], [20], [24], [0]\} \\ \langle [7] \rangle &= \{[0], [7], [14], [21]\} \\ \langle [14] \rangle &= \{[14], [0]\} \\ \langle [28] \rangle &= \langle [0] \rangle = \{[0]\} \end{aligned}$$

Problem 5. *(5pts) Let G be an abelian group and $H = \{g \in G | g^2 = e\}$, where e is the identity element of G. Show that H is a subgroup of G.*

Solution. Since $e^2 = ee = e$, we have $e \in H$: the identity is in H.

Let $a, b \in H$, so that $a^2 = e$ and $b^2 = e$. To show that H is closed under multiplication, consider $(ab)^2$. Since G is abelian, we have

$$(ab)^2 = abab = aabb = a^2b^2 = ee = e,$$

so $ab \in H$. Thus H is closed.

Let $a \in H$, so that $a^2 = e$, and let a^{-1} be the inverse of a. Consider

$$a^{-1}a^{-1} = (a^{-1})^2 = (a^2)^{-1} = e^{-1} = e,$$

so $a^{-1} \in H$.

Therefore, H is a subgroup of G.

Problem 6. *(10pts)*

(a) Let G be a group. For $a \in G$, define a mapping $t_a : G \longrightarrow G$ by $t_a(x) = axa^{-1}$ for all $x \in G$. Prove that t_a is an isomorphism.

(b) i)Prove that $\mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_3$.
ii) Prove that $\mathbb{Z}_6$ is not isomorphic to S_3, where S_3 is the group of permutations on the set $\{1, 2, 3\}$.

Solution. (a) If $x, y \in G$, then

$$t_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = t_a(x) \cdot t_a(y).$$

So, t_a is a homomorphism. Now let $x, y \in G$ and $t_a(x) = t_a(y)$. Then $axa^{-1} = aya^{-1}$. Since G is a group, it allows left and right cancellation. Therefore $x = y$. So, t_a is one-to-one. Finally, let $x \in G$. We shall show that there is y in G such that $t_a(y) = x$. Let $y = a^{-1}xa$. Then

$$t_a(y) = t_a(a^{-1}xa) = aa^{-1}xaa^{-1} = x.$$

So, $t_a(x)$ is onto. Hence, $t_a(x)$ is an isomorphism.

(b) i) Since their orders are different, $|\mathbb{Z}_2| = 2 \neq 3 = |\mathbb{Z}_3|$, we cannot find a bijection between the sets, so the groups cannot be isomorphic.

ii) $\mathbb{Z}_6$ is an abelian group, but S_3 is not. Under an isomorphism being abelian must be preserved: $\phi(xy) = \phi(yx)$ since $xy = yx$, so

$$\phi(x) \cdot \phi(y) = \phi(xy) = \phi(yx) = \phi(y) \cdot \phi(x).$$

Remark. In the last part, it would be acceptable to note that $\mathbb{Z}_6$ is cyclic, but S_3 is not.