HW2 SOLUTION

JI ZENG

Only problems with provided solutions will be graded. Solutions might be concise for some problems, but please be noticed that they don't reflect the wanted level of detailedness of your answer.

Armstrong.2.7
Multiply x^{-1} (it exists in G as G is a group) to the right of both sides of $wx = y$ we obtain

$$(wx)x^{-1} = yx^{-1} \implies w = yx^{-1}.$$

And similarly, multiply x^{-1} to the left of both sides of $xz = y$ we obtain $z = x^{-1}y$. So both w and z exists and is unique.

Armstrong.3.4
Write $G_n := \{x \in \mathbb{C}; x^n = 1\}$ and $G = \cup_{n\in\mathbb{N}} G_n$. We'd like to check that G under complex multiplication is a group.
Firstly we need to show that G is closed under multiplication, i.e. $\forall a, b \in G$ we need $ab \in G$. Indeed, for arbitrary $a, b \in G$ we have some m, n s.t. $a \in G_m$ and $b \in G_n$, and this means $a^m = 1$, $b^n = 1$. So $a^{mn} = (a^m)^n = 1^n = 1$, which means $a \in G_{mn}$. Similarly $b \in G_{mn}$ and we checked that G_{mn} is a group under complex multiplication in Armstrong.3.3, so $ab \in G_{mn} \subset G$.
Then we need to show the multiplication is associative, but this is obvious because complex multiplication is associative. Also we need to show that there exists an identity, but this is again trivial because $1 \in G$.
Finally we need to show the existence of inverses. For arbitrary $a \in G$, we know there's some n s.t. $a \in G_n$. So as we checked that G_n is a group in Armstrong.3.3, so $a^{-1} \in G_n \subset G$.

Problem.A
(a) Injectivity: Suppose that $r_a(x) = r_a(y)$, which means $x * a = y * a$. As G is a group, we can multiply a^{-1} to the both sides from the right and we obtain

$$(x * a) * a^{-1} = (y * a) * a^{-1} \implies x = y,$$

which means r_a is injective.
Surjectivity: Choose arbitrary $z \in G$, we'd like to find $x \in G$ s.t. $r_a(x) = z$. Simply take $x = z * a^{-1}$, then $r_a(x) = (z * a^{-1}) * a = z$ as wanted.
(b) Take arbitrary x, we'd like to show $r_{a*b}(x) = r_b \circ r_a(x)$. Indeed,

$$\begin{aligned} r_b \circ r_a(x) &= r_b(r_a(x)) \\ &= r_b(x * a) = (x * a) * b = x * (a * b), \text{ by associativity} \\ &= r_{a*b}(x), \end{aligned}$$

as wanted.

Problem.C

(a) By definition $\mathbb{Z}_{43}^* = \{[n] \in \mathbb{Z}_{43}; gcd(n, 43) = 1\}$. Because 43 is prime, every integer is coprime to it, so $|\mathbb{Z}_{43}^*| = 42$.
(b) $[2] \cdot [5] = [2 \cdot 5] = [10]$.
$[3] \cdot [17] = [3 \cdot 17] = [51] = [8]$.
$[11] \cdot [13] = [11 \cdot 13] = [143] = [14]$.
$[-7] \cdot [19] = [-7 \cdot 19] = [-133] = [39]$.
(c) Because $gcd(41, 43) = 1$, so $[41] \in \mathbb{Z}_{43}^*$. Now we use Euclid's algorithm to find $x, y \in \mathbb{Z}$ s.t. $x \cdot 41 + y \cdot 43 = 1$.
Indeed $gcd(41, 43) = gcd(41, 2) = gcd(1, 2) = 1$, and use back-substitution

$$1 = 41 - (20 \cdot 2) = 41 - 20 \cdot (43 - 41) = 21 \cdot 41 - 20 \cdot 43.$$

So $21 \cdot 41 \equiv 1 \pmod{43}$ which means $[21]$ is the inverse of $[41]$.

Problem.D

(a) We have prime factorization $385 = 5 * 7 * 11$. By property of the totient function

$$\begin{aligned}\phi(385) &= \phi(5)\phi(7)\phi(11) \\ &= (5-1)(7-1)(11-1) = 240.\end{aligned}$$

(b) A general solution to $x \equiv 1 \pmod 5$ is $x = 5n + 1$ for $n \in \mathbb{Z}$.
In order to have $x \equiv 2 \pmod 7$, we need $5n + 1 \equiv 2 \pmod 7$, which is equivalent to $5n \equiv 1 \pmod 7$. We can compute the inverse of $[5]$ in $\mathbb{Z}_7^*$ is $[3]$. So $n \equiv 2 \pmod 7$. A general solution to n is $n = 7m + 3$ and so $x = 35m + 16$.
Additionally we want $x \equiv 3 \pmod{11}$, we need $35m + 16 \equiv 3 \pmod{11}$, which is equivalent to $35m \equiv 9 \pmod{11}$. We can compute the inverse of $[35] = [2]$ in $\mathbb{Z}_{11}^*$ is $[6]$. So $m \equiv 9 * 6 \equiv 10 \pmod{11}$. So m has general solution $m = 11t + 10$. Hence $x = 35m + 16 = 385t + 366$ $t \in \mathbb{Z}$ is the general solution we want.
(c) For $t = 0$, $x = 385$. For $n > 0$, $|x| > 400$. For $n = -1$, $x = -19$. For $n < -1$, $|x| > 400$.