Homework 1

Due: May 15th (Saturday), 11:59 pm

- Please submit your work on Blackboard.
- You are required to submit your work as a single pdf, not as an email attachment (if needed, there are many online converters of jpg pictures to pdfs).
- Please make sure your handwriting is clear enough to read. Thanks.
- No late work will be accepted.
- There are five randomly picked questions (2 pts for each) that will be graded. (1), (2), (4), (7), (8)

---

(0) Read §1.1 and §1.2 to make sure you understand the gcd, lcm, and Euclidean algorithm.

(1) Solve the following congruences.

(a) $2x \equiv 1 \pmod 9$ $\quad d = (2,9) = 1|1\checkmark \Rightarrow \boxed{x \equiv 5 \pmod 9}$

(b) $20x \equiv 12 \pmod{72}$ $\quad d = (20,72) = 4|12\checkmark \Rightarrow 5x \equiv 3 \pmod{18}$
Solve $5x \equiv 1 \pmod{18}$ first: $x \equiv 11 \pmod{18}$.
Thus, $5x \equiv 3 \pmod{18} \Rightarrow x \equiv 33 \equiv 15 \pmod{18}$
Equivalently, $\boxed{x \equiv 15, 33, 51, 69 \pmod{72}}$

(2) Solve the following system of congruences.

$$x \equiv 15 \pmod{27} \qquad x \equiv 16 \pmod{20}$$

$$\begin{bmatrix}1 & 0 & 27\\ 0 & 1 & 20\end{bmatrix} \rightsquigarrow \begin{bmatrix}1 & -1 & 7\\ 0 & 1 & 20\end{bmatrix} \rightsquigarrow \begin{bmatrix}1 & -1 & 7\\ -2 & 3 & 6\end{bmatrix} \rightsquigarrow \begin{bmatrix}3 & -4 & 1\\ -2 & 3 & 6\end{bmatrix} \rightsquigarrow \begin{bmatrix}3 & -4 & 1\\ -20 & 27 & 0\end{bmatrix}$$

Therefore, $3 \cdot 27 + (-4) \cdot 20 = 1$. By CRT, we take

$$x \equiv 16(3 \cdot 27) + 15((-4) \cdot 20) \pmod{27 \cdot 20} \Rightarrow \boxed{x \equiv 96 \pmod{540}}$$

(3) Make addition and multiplication tables for $\mathbf{Z}_4$.

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

·	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

(4) Find the multiplicative inverses of the given elements (if possible).

(a) $[6]$ in $\mathbf{Z}_{15}$. No multiplicative inverse since $(6, 15) = 3 \neq 1$

(b) $[7]$ in $\mathbf{Z}_{15}$. $[7][2] = [-1] \Rightarrow [7][-2] = [7][13] = [1] \Rightarrow \boxed{[7]^{-1} = [13]}$

(5) Let $(a, n) = 1$. The smallest positive integer k such that $a^k \equiv 1 \pmod{n}$ is called the **multiplicative order** of $[a]$ in $\mathbf{Z}_n^\times$.
Find the multiplicative orders of [5] and [7] in $\mathbf{Z}_{16}^\times$ and show that their multiplicative orders both divide $\varphi(16)$. $\varphi(16) = 8$.
$[5]^2 = [25] = [9], [5]^3 = [5]^2[5] = [45] = [-3], [5]^4 = [5]^3[5] = [-15] = [1]$
$\Rightarrow$ order is $4|\varphi(16)$. ✓
$[7]^2 = [49] = [1] \Rightarrow$ order is $2|\varphi(16)$. ✓

(6) Consider the following permutations in S_7.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 6 & 1 & 7 \end{pmatrix} \qquad \text{and} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 7 & 4 & 6 & 3 \end{pmatrix}$$

(a) Write the following permutations as a product of disjoint cycles.

(i) $\sigma\tau$ (ii) $\tau\sigma$ (iii) σ^{-1} (iv) $\sigma\tau\sigma^{-1}$

Write $\sigma = (1356)$ and $\tau = (12)(3547)$.
(i) $\sigma\tau = (1356)(12)(3547) = (1236)(475)$
(ii) $\tau\sigma = (12)(3547)(1356) = (1562)(347)$
(iii) $\sigma^{-1} = (6531) = (1653)$
(iv) $\sigma\tau\sigma^{-1} = (\sigma\tau)\sigma^{-1} = (1236)(475)(1653) = (1)(23)(4756) = (23)(4756)$

(b) Write σ and τ as products of transpositions.
$\sigma = (1356) = (56)(36)(16) = (13)(35)(56)$
$\tau = (12)(3547) = (12)(47)(57)(37) = (12)(35)(54)(47)$

(7) Write

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 10 & 5 & 7 & 8 & 2 & 6 & 9 & 1 \end{pmatrix}$$

as a product of disjoint cycles and as a product of transpositions. Find its inverse, and find its order.
$(1\,3\,\mathbf{10})(2457)(68) = (13)(3\,\mathbf{10})(24)(45)(57)(68) = (3\,\mathbf{10})(1\,\mathbf{10})(57)(47)(27)(68)$
Order$=\operatorname{lcm}[3, 4, 2] = 12$. Inverse is $(\mathbf{10}\,3\,1)(7542)(86) = (1\,\mathbf{10}\,3)(2754)(68)$

(8) Find the order of each of the following permutations.
Hint: First write each permutation as a product of disjoint cycles.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 7 & 5 & 1 & 8 & 2 & 3 \end{pmatrix}$

$(145)(26837) \Rightarrow$ Order$=\operatorname{lcm}[3, 5] = 15$.

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 8 & 7 & 3 & 4 & 6 & 1 & 2 \end{pmatrix}$

$(1538)(29)(476) \Rightarrow$ Order$=\operatorname{lcm}[4, 2, 3] = 12$.