September 30, 2024

Problem Set 3 Solutions

Exercise 1. Determine which of the following groups are cyclic.

(a) $(\mathbb{Z}/12\mathbb{Z})^*,\ \cdot)$

(b) $(\mathbb{Z}/12\mathbb{Z}, +)$

(c) $((\mathbb{Z}/8\mathbb{Z})^*,\ \cdot)$

Solution 1. (a) The group $(\mathbb{Z}/12\mathbb{Z})^*,\ \cdot)$ is not cyclic. Observe that $G = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$ and that $5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \mod 12$. Therefore none of the elements of the group can be a generator.

(b) The group $G = (\mathbb{Z}/12\mathbb{Z}, +)$ is cyclic. Observe that the element $[1]_{12}$ with the operation sum can generate every element of the group.

(c) The group $G = ((\mathbb{Z}/8\mathbb{Z})^*,\ \cdot)$ is not cyclic. Note that $G = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ and that $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \mod 8$. Therefore none of these elements can generate G.

Remark: It is easy to see that for any prime p the group $((\mathbb{Z}/p\mathbb{Z})^*,\ \cdot)$ is cyclic. More generally, there is the following result (that we cite here without a proof):

Theorem (Gauss)**.** The group $((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot)$ is cyclic if and only if $n = 2, 4$, any power of an odd prime or twice any power of an odd prime.

Exercise 2. For each of the groups below, find the order of the element $g \in G$;

(a) $G = ((\mathbb{Z}/20\mathbb{Z})^*,\ \cdot)$, $g = [3]_{20}$.

(b) $G = ((\mathbb{Z}/24\mathbb{Z})^*, \cdot)$, $g = [5]_{24}$ and $g = [11]_{24}$.

(c) $G = \mathrm{GL}_2(\mathbb{R})$, $g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$.

Solution 2. (a) Note that $3^4 = 81$, then $3^4 \equiv 1 \mod 20$. Also $([3]_{20})^j \neq [1]_{20}$ for $j = 1, 2, 3$. Thus $[3]_{20}$ has order 4.

(b) Observe that $5^2 = 25$ and $11^2 = 121$, then $5^2 \equiv 1 \mod 24$ and $11^2 \equiv 1 \mod 24$. Thus both $[5]_{24}$ and $[11]_{24}$ have order 2.

(c) The element $g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ has order 4:

$$g^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$g^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$g^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Consider the element $g = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. For any $n \in \mathbb{Z}^+$ we compute:

$$\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -n-1 \\ 0 & 1 \end{pmatrix}.$$

Therefore, for any $n \in \mathbb{Z}^+$ we have $g^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \neq e$. The element g has infinite order in $G = \mathrm{GL}_2(\mathbb{R})$.

Exercise 3. (a) Find the last digit of 7^{1000}.

(b) Show that 72 divides $53^{48} - 1$.

(c) Show that the number $a = (29^{16} + 28^{16})(29^8 + 28^8)(29^4 + 28^4)(29^2 + 28^2)(29 + 28)$ is divisible by 51.
Hint: Use Euler's theorem.

Solution 3. (a) By Euler's theorem, $a^{\varphi(n)} \equiv 1 \pmod{n}$ for any $a \in \mathbb{N}$ coprime to $n \in \mathbb{Z}_+$. We have $\varphi(10) = 4$, and therefore $7^4 \equiv 1 \pmod{10}$. Then we obtain $(7^4)^{250} \equiv 1 \pmod{10} = 7^{1000} \equiv 1 \pmod{10}$. The last digit is 1.

(b) We use the prime factorization of $72 = 2^3 \cdot 3^2$. We have $\varphi(2^3) = 2^3 - 2^2 = 4$, $\varphi(3^2) = 3^2 - 3 = 6$. As 53 is prime, by Euler's theorem we have $53^4 \equiv 1 \pmod{8}$ and $53^6 \equiv 1 \pmod{9}$. Therefore, $53^{48} \equiv 1 \pmod{8}$ and $53^{48} \equiv 1 \pmod{9}$. Since $53^{48} - 1$ is divisible by both 8 and 9, it is divisible by 72.

(c) Note that $51 = 3 \cdot 17$. First, $29 + 28 = 57 = 3 \cdot 19$, so a is divisible by 3. Now we can write

$$a = a(29 - 28) = (29^{16} + 28^{16})(29^8 + 28^8)(29^4 + 28^4)(29^2 + 28^2)(29 + 28)(29 - 28) =$$

$$= (29^{16} + 28^{16})(29^8 + 28^8)(29^4 + 28^4)(29^2 + 28^2)(29^2 - 28^2) = (29^{16} + 28^{16})(29^8 + 28^8)(29^4 + 28^4)(29^4 - 28^4) =$$

$$= (29^{16} + 28^{16})(29^8 + 28^8)(29^8 - 28^8) = (29^{16} + 28^{16})(29^{16} - 28^{16}) = 29^{32} - 28^{32}.$$

By Euler's theorem we have $29^{16} \equiv 1 \pmod{17}$ and $28^{16} \equiv 1 \pmod{17}$, therefore $29^{32} \equiv 28^{32} \pmod{17}$, and $a = 29^{32} - 28^{32}$ is divisible by 17. Finally, a is divisible by $3 \cdot 17 = 51$.

Exercise 4. (a) Show that $a^{13} \equiv a \pmod{2730}$ for any integer a.

(b) Let q and p be two distinct primes. Show that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

(c) Let p be a prime different from 2 and 5. Show that p divides an infinite number of elements of the sequence $9, 99, 999, 9999, \ldots$. (Hint: note that each element of the sequence can be written as $10^a - 1$ for an integer a.)

Solution 4. (a) This is equivalent to proving that 2730 divides $a - a^{13}$, for every value $a \in \mathbb{Z}$. First, observe that we can write 2730 as the product of the following prime values $2730 = 13 \cdot 5 \cdot 7 \cdot 3 \cdot 2$. We will show that each of these prime factors divides $a - a^{13}$, for any $a \in \mathbb{Z}$, i.e. $a^{13} \equiv a \pmod{p}$ for $p = 2, 3, 5, 7, 13$.

By Fermat's little theorem we have $a^p \equiv a \pmod{p}$ for any integer a. So for $p = 13$, $a^{13} \equiv a \pmod{13}$, as desired.

For $p = 7$, $a^{13} = a^7 a^6$ et $a^7 a^6 \equiv aa^6 \pmod{7}$. So we have $a^{13} \equiv a^7 \pmod{7}$, and again by Fermat: $a^{13} \equiv a \pmod{7}$.

Similarly for $p = 5$: $a^{13} = a^5 a^5 a^3$. So $a^{13} \equiv aaa^3 \pmod{5}$ and then further $a^5 \equiv a \pmod{5}$, as desired.

The arguments for 2 and 3 are entirely similar.

(b) By Fermat's Little Theorem $p^{q-1} \equiv 1 \mod q$. This implies that $p^{q-1} + q^{p-1} \equiv 1 \mod q$. Similarly, $p^{q-1} + q^{p-1} \equiv 1 \mod p$. Therefore p and q both divide $(p^{q-1} + q^{p-1} - 1)$. This means that $\mathrm{lcm}(p, q)$ divides $(p^{q-1} + q^{p-1} - 1)$. Now, $\mathrm{lcm}(p, q) = p \cdot q$. Thus we can conclude that $p^{q-1} + q^{p-1} \equiv 1 \mod pq$.

(c) Observe that the n-th term in the sequence $\{9, 99, 999, 9999 \ldots\}$ can be written as $a_n = 10^n - 1$. Let p be a prime other than 2 or 5. We have that $a_n \equiv 0 \mod p$ if and only if $10^n \equiv 1 \mod p$. Then, by Fermat's Little Theorem we can find infinitely many $n = k(p-1)$ so that $10^n = (10^{p-1})^k \equiv 1^k \equiv 1 \mod p$.

Exercise 5. Let C_n denote the cyclic group of order $n \in \mathbb{Z}^+$.

(a) Describe all group homomorphisms $C_n \to C_n$. How many are there?

(b) The kernel of a group homomorphism $C_n \to C_n$ is the set of the elements of C_n that are mapped to 1. A homomorphism from a group to itself is an automorphism if its kernel is trivial (equal to $\{1\}$). Describe all group automorphisms $C_n \to C_n$. How many are there?

(c) Describe all group homomorphisms $C_n \to C_m$ for $m, n \in \mathbb{Z}^+$, $m \neq n$. How many are there?

Solution 5. (a) The cyclic group C_n is presented in generators and relations as $C_n = \langle t \,|\, t^n = 1 \rangle$. A group homomorphism $\phi : C_n \to C_n$ is defined by assigning $\phi(t) = t^k$, where k is an integer considered modulo n. The only condition to check is that $\phi(t^n) = (\phi(t))^n = t^{kn} = 1$. Since $t^n = 1$, this condition is satisfied for any k. Therefore, there are n different homomorphisms $\phi : C_n \to C_n$ defined by $\phi(t) = t^k$, $k = 0, 1, \ldots n-1$.

(b) To ensure that $\phi : C_n \to C_n$ is an automorphism, we need to check that the kernel of ϕ is trivial. This means that we are looking for the homomorphisms $\phi(t) = t^k$ such that $\phi(t^i) = t^{ki} \neq 1$ for all $i = 1, \ldots n-1$. This is equivalent to the condition that n does not divide ik for all $i = 1, \ldots n-1$, which holds if and only if k is coprime with n. Therefore, the number of distinct automorphisms of C_n is equal to the value of Euler's totient function $\varphi(n)$.

(c) Let $\phi : C_n \to C_m$ be a group homomorphism. It is defined by assigning $\phi(t) = q^i$, where $t : t^n = 1$ and $q : q^m = 1$ are generators of the groups C_n and C_m respectively. The condition to check for ϕ to be a homomorphism is $(\phi(t))^n = q^{in} = 1$. This happens if and only if m divides the product in. We have $mk = in$ for some integer k. Let $d = \gcd(m, n)$. This is equivalent to

$$k\frac{m}{d} = i\frac{n}{d}$$

for some integer k. Since $\frac{m}{d}$ and $\frac{n}{d}$ are relatively prime, the condition on i is that it has to be a multiple of $\frac{m}{d}$. Since i are integers modulo m, we obtain the following different choices for i:

$$i = \{0, \frac{m}{d}, \frac{2m}{d}, \ldots \frac{(d-1)m}{d}\}$$

Finally, there exists $\gcd(m, n)$ distinct group homomorphisms $\phi : C_n \to C_m$. Note that the answer is symmetric with respect to the swap $m \leftrightarrow n$. The number of group homomorphisms $\psi : C_m \to C_n$ is the same.