Midterm I Solutions

Problem 1.

(i) Find the inverse of 11 in $\mathbb{Z}_{37}$.

(ii) Show that
$$a^{40} \equiv 1 \mod 451$$
whenever $\gcd(a, 451) = 1$.

`Solution:`

(i) *Let x be the inverse of 11 in $\mathbb{Z}_{37}$. By definition*
$$11x \equiv 1 \mod 37 \implies 11x = 1 + 37y$$
for some integer y. We obtain
$$11x + 37(-y) = 1.$$
We find a solution of this congruence by the division algorithm. Indeed,
$$37 = 11 \cdot 3 + 4$$
$$11 = 4 \cdot 2 + 3$$
$$4 = 3 \cdot 1 + 1.$$
In reverse, we have
$$1 = 4 - 3 \cdot 1 = 4 - (11 - 4 \cdot 2) = 4 \cdot 3 - 11 \cdot 1 = (37 - 11 \cdot 3) \cdot 3 - 11 \cdot 1 = 37 \cdot 3 - 11 \cdot 10.$$
We conclude that a solution is
$$x = -10, -y = 3.$$
Thus, the inverse of 11 in $\mathbb{Z}_{37}$ equals
$$-10 \mod 37 \equiv 27 \mod 37.$$

(ii) *We have $451 = 11 \cdot 41$. Thus $\gcd(a, 451) = 1 \implies \gcd(a, 11) = 1$ and $\gcd(a, 41) = 1$. Applying Fermat's theorem for the primes $p = 11$ and $p = 41$ we have*
$$a^{10} \equiv 1 \mod 11 \implies a^{40} \equiv 1 \mod 11$$
$$a^{40} \equiv 1 \mod 41.$$
Thus $a^{40} - 1$ is divisible by both 11 and 41, hence by their product $11 \cdot 41$, since $\gcd(11, 41) = 1$. This implies
$$a^{40} \equiv 1 \mod 451.$$

Problem 2.

Consider the permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 6 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 4 & 5 & 2 \end{pmatrix}.$$

(i) Find the permutation χ such that

$$\sigma\chi = \tau.$$

(ii) Determine the parity of σ and τ.

(iii) Show that there are no permutations μ such that $\sigma^5 = \mu^2\tau$.

`Solution:`

(i) *We have*

$$\sigma\chi = \tau \implies \sigma^{-1}\sigma\chi = \sigma^{-1}\tau \implies \chi = \sigma^{-1}\tau.$$

We compute

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix}$$

and therefore

$$\chi = \sigma^{-1}\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 4 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 2 & 1 & 3 \end{pmatrix}$$

(ii) *We first write σ as product of cycles*

$$\sigma = (1\,5\,6)(2\,4\,3).$$

From here, using that

$$(a\,b\,c) = (a\,b)(b\,c)$$

we conclude

$$\sigma = (1\,5)(5\,6)(2\,4)(4\,3).$$

Since 4 *transpositions are used, it follows that σ is an even permutation. We note that*

$$\tau = (1\ 6\ 2\,3) = (1\ 6)(6\ 2)(2\ 3).$$

Since 3 *transpositions are used, τ is an odd permutation.*

(iii) *We have two cases:*

- *if μ is even, then σ^5 is even being product of even permutations, while $\mu^2\tau$ is odd being product of two even and one odd permutation.*
- *if μ is odd, then σ^5 is even, while $\mu^2\tau$ is odd being product of three odd permutations.*

In both cases $\sigma^5 \neq \mu^2\tau$ since the parities are different.

Problem 3.

(i) Consider the permutation

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

Write σ as product of three disjoint cycles $\gamma_1, \gamma_2, \gamma_3$.

(ii) Compute $\gamma_1^{60}, \gamma_2^{60}, \gamma_3^{60}$.

(iii) Using (i) and (ii), compute σ^{60}.

`Solution:`

(i) *We have*

$$\sigma = (1\ 7\ 3\ 10\ 4)\,(2\ 9)(5\ 8\ 6).$$

We write

$$\gamma_1 = (1\ 7\ 3\ 10\ 4),\ \ \gamma_2 = (2\ 9),\ \ \gamma_3 = (5\ 8\ 6).$$

(ii) *We note that for a cycle of length ℓ, its ℓ^{th} power equals the identity; this is because each member is sent to the one following it successively ℓ times, so at the end it will cycle through to the starting point.*

In particular,

$$\begin{aligned} \gamma_1^5 = \epsilon &\implies \gamma_1^{60} = (\gamma_1^5)^{12} = \epsilon \\ \gamma_2^2 = \epsilon &\implies \gamma_2^{60} = (\gamma_2^2)^{30} = \epsilon \\ \gamma_3^3 = \epsilon &\implies \gamma_3^{60} = (\gamma_3^3)^{30} = \epsilon. \end{aligned}$$

(iii) *We know that disjoint cycles commute so*

$$\gamma_i \gamma_j = \gamma_j \gamma_i.$$

We have

$$\sigma^{60} = (\gamma_1\gamma_2\gamma_3)^{60} = \gamma_1\gamma_2\gamma_3 \cdots \gamma_1\gamma_2\gamma_3 = \gamma_1^{60}\gamma_2^{60}\gamma_3^{60}.$$

Here we used that the γ's commute so the order does not matter: this way we moved all the γ_1's to the left, all the γ_2's to the middle, and the γ_3's at the end.

Using (ii), we find

$$\sigma^{60} = \gamma_1^{60}\gamma_2^{60}\gamma_3^{60} = \epsilon \cdot \epsilon \cdot \epsilon = \epsilon.$$

Problem 4.

(i) If χ and τ are two permutations in S_n, show that the inverse of the permutation $\chi\tau$ is the permutation $\chi^{-1}\tau^{-1}$. In symbols,

$$(\chi\tau)^{-1} = \tau^{-1}\chi^{-1}.$$

(ii) On the set S_n of permutations define $\sigma_1 \sim \sigma_2$ if there exists a permutation τ such that

$$\sigma_1 = \tau\sigma_2\tau^{-1}.$$

Show that $\sim$ defines an equivalence relation on the set S_n of permutations.

`Solution:`

(i) *Write $\nu = \chi\tau$ and $\mu = \tau^{-1}\chi^{-1}$. To show that μ is the inverse of the permutation ν we compute*

$$\mu\nu = \nu\mu = \epsilon.$$

Indeed,

$$\mu\nu = \tau^{-1}\chi^{-1}\chi\tau = \tau^{-1}\epsilon\tau = \tau^{-1}\tau = \epsilon$$

and similarly

$$\nu\mu = \chi\tau\tau^{-1}\chi^{-1} = \chi\epsilon\chi^{-1} = \chi\chi^{-1} = \epsilon.$$

(ii) *We show that $\sim$ is reflexive, symmetric and transitive.*

- *Reflexive: we show $\sigma \sim \sigma$. Indeed, letting $\tau = \epsilon$, we have*

$$\sigma = \tau\sigma\tau^{-1} \implies \sigma \sim \sigma.$$

- *Symmetric: we show $\sigma_1 \sim \sigma_2 \implies \sigma_2 \sim \sigma_1$. Indeed,*

$$\sigma_1 = \tau\sigma_2\tau^{-1}$$

for some τ. We solve

$$\sigma_2 = \tau^{-1}\sigma_1\tau.$$

Let $\mu = \tau^{-1}$ so that $\mu^{-1} = \tau$. Then

$$\sigma_2 = \tau^{-1}\sigma_1\tau = \mu\sigma_1\mu^{-1} \implies \sigma_2 \sim \sigma_1.$$

- *Transitive: we show*

$$\sigma_1 \sim \sigma_2,\ \sigma_2 \sim \sigma_3 \implies \sigma_1 \sim \sigma_3.$$

Indeed, by definition

$$\sigma_1 = \tau\sigma_2\tau^{-1}$$

for some τ. Similarly,

$$\sigma_2 = \chi\sigma_3\chi^{-1}$$

for some χ. Then

$$\sigma_1 = \tau\sigma_2\tau^{-1} = \tau\chi\sigma_3\chi^{-1}\tau^{-1} = (\tau\chi)\sigma_3(\tau\chi)^{-1}$$

where part (i) was used in the last line. Setting $\mu = \tau\chi$*, we therefore have*

$$\sigma_1 = \mu\sigma_3\mu^{-1}$$

showing $\sigma_1 \sim \sigma_3$*.*

Problem 5.

(i) Let $p > 2$ be a prime. Prove Wilson's theorem stating that

$$(p-1)! \equiv -1 \mod p.$$

(ii) Let n be a positive integer, and let π denote the product of all units in $\mathbb{Z}_n$. Show that

$$\pi^2 \equiv 1 \mod n.$$

`Solution:`

(i) *Since p is a prime, every $x \in \{1, 2, \ldots, p-1\}$ must be invertible in $\mathbb{Z}_p$. We write x^{-1} for the inverse. In the product*

$$(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$$

the elements come in pairs (x, x^{-1}). The elements in each pair multiply to 1 in $\mathbb{Z}_p$. If $x \neq x^{-1}$ in $\mathbb{Z}_p$, each pair contributes 1 to $(p-1)!$. It can happen however that $x = x^{-1}$ in $\mathbb{Z}_p$. This means

$$x \equiv x^{-1} \mod p \implies x^2 \equiv 1 \mod p \implies p | x^2 - 1 = (x-1)(x+1)$$
$$\implies p | x - 1 \textit{ or } p | x + 1 \implies x \equiv \pm 1 \mod p.$$

Therefore the only elements which are unaccounted for in the product $(p-1)!$ are 1 and $p-1$, which together multiply to $-1 \mod p$. Thus

$$(p-1)! \equiv -1 \mod p.$$

(ii) *The reasoning is similar. Let $u_1, \ldots, u_k$ be the invertible elements in $\mathbb{Z}_n$ so that*

$$\pi = u_1 \cdot \ldots \cdot u_k.$$

In this product, we pair up each x with its inverse x^{-1}. The elements in each pair multiply to 1 in $\mathbb{Z}_n$. There will however be units x which equal their inverse x^{-1}. Say these units are $v_1, \ldots, v_\ell$. Then

$$\pi = v_1 \cdots v_\ell.$$

However,

$$x = x^{-1} \textit{ in } \mathbb{Z}_n \implies x^2 = 1 \textit{ in } \mathbb{Z}_n$$

so in particular $v_i^2 = 1$ in $\mathbb{Z}_n$. Then

$$\pi^2 = (v_1 \cdots v_\ell)^2 = v_1^2 \cdots v_\ell^2 = 1$$

in $\mathbb{Z}_n$.

Extra credit.

Show that there are infinitely many primes p which are of the form $4k+1$.

Hint: Consider $A = (2p_1 \cdots p_n)^2 + 1$.

`Solution:` *Assume for a contradiction that there are only finitely many primes $p_1, \ldots, p_n$ of the form $4k+1$. Set*

$$A = (2p_1 \cdots p_n)^2 + 1.$$

Note that $A > 1$. Let q be a prime divisor of A. Then

$$(2p_1 \cdots p_n)^2 + 1 \equiv 0 \mod q$$

and therefore the equation

$$x^2 + 1 \equiv 0 \mod q$$

has the solution $x = 2p_1 \ldots p_n$. By a result in class, this shows that $q = 2$ or $q \equiv 1 \mod 4$. However, A is odd, so q must be odd as well. Hence $q \neq 2$. Thus $q \equiv 1 \mod 4$. Therefore, q is a prime of the form $4k+1$, so it must be one of the primes on our list $p_1, \ldots, p_n$. Thus $q = p_i$ for some i. We obtain

$$q|A \implies p_i|A \implies A \equiv 0 \mod p_i.$$

This is however impossible since

$$A = (2p_1 \cdots p_n)^2 + 1 \equiv 1 \mod p_i \implies A \not\equiv 0 \mod p_i.$$

Therefore, our assumption was wrong and there must be infinitely many primes of the form $4k+1$.