# COMP6453 Tutorial Week 5 Solutions

## 1 Fast Computations

(i). Compute $17^{10} \pmod{2023}$ using repeated squaring.

**Answer:**

$17^2 = 289 \pmod{2023}$

$289^2 = 17^4 = 578 \pmod{2023}$

$578^2 = 17^8 = 289 \pmod{2023}$

$17^{10} = 17^8 \cdot 17^2 = 289 \cdot 289 = 578 \pmod{2023}$

(ii). Use the extended Euclidean algorithm to compute the multiplicative inverse of 9 modulo 26.

**Answer:**

$26 = 2 \times 9 + 8$

$9 = 1 \times 8 + 1$

$1 = 9 \times 8(1)$

$8 = 26 - 9(2)$

$1 = 9 - 8(1) \implies 1 = 9 - (26 - 9(2))(1) \implies 9(3) - 26 = 1$

This tells us the inverse of 9 mod 26 is 3 (this is to be expected as $9 \cdot 3 = 27 = 1 \pmod{26}$).

## 2 Euler $\phi$ Function

(i). Show the $\phi$ function is multiplicative. That is, show $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ where $gcd(a, b) = 1$.

**Answer:**

If $gcd(a, b) = 1$, the Chinese Remainder Theorem says that the mapping $\phi : Z_{ab} \to Z_a \times Z_b$ via $x \mapsto (x \pmod{a}, x \pmod{b})$. This restricts to an isomorphism from the multiplicative unit groups $(Z_{ab})^* \to Z_a^* \times Z_b^*$. The theorem follows because $|(Z_k)^*| = \phi(k)$ for any number $k$.

(ii). Let $n \in \mathbb{N}$ have prime factorization $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Show $\phi(n) = (p_1^{e_1} - p_1^{e_1 - 1}) \dots (p_k^{e_k} - p_k^{e_k - 1})$.

**Answer:**

If we can show that for any number $k$ and prime $p$, $\phi(p^k) = (p-1) \cdot p^{k-1}$, we are done by part (i). The set $a \in \{0, ..., p^k\}$ such that $gcd(a, p^k) > 1$ is precisely the set $\{p, 2p, ..., p^{k-1}p\}$. This set has size $p^{k-1}$. Therefore, the size of the set of numbers smaller than $p^k$ and coprime to $p^k$ is $p^k - p^{k-1}$.

# 3 Polynomial Evaluation

Write an efficient algorithm that takes a polynomial $P(x)$ of degree $d$ and evaluates it at a point $a$ to find $P(a)$. What is the time complexity of the algorithm?

**Answer:**

Using Horner's rule, this can be done in O(d) time.

# 4 Karatsuba Multiplication

Revisit Karatsuba algorithm.

**Answer:**

We have $12 = 10 \cdot 1 + 2$ and $14 = 10 \cdot 1 + 4$. We recurse and call $U = Karatsuba(1, 1) = 1$, $V = Karatsuba(2, 4) = 8$, $W = Karatsuba(1 - 2, 1 - 4) = Karatsuba(-1, -3) = 3$. Now we compute $Z = U + V - W = 6$. The answer is given by $P = 10^2U + 10Z + V = 100 + 60 + 8 = 168$.