COMP6453 Tutorial Week 5

1 Fast Computations

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

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

2 Euler ϕ Function

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

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

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?

4 Karatsuba Multiplication

Revisit Karatsuba algorithm.