Dheeraj Satya Sushant Viswanadham
(z5204820)

COMP3121 Assignment 2 – Question 2

2) We have $P(x) = A_0 + A_1x^{100} + A_2x^{200}$ where A_1, A_2 and A_3*a*re arbitrarily large numbers. We are required to square *P(x)* using only 5 large integer multiplications.

We must recognise that using the naïve implementation, we see that P(x) has degree of 200 and by squaring it, we would need (200 + 200 + 1) 401 values to evaluate it which is greater than our limit of 5 multiplications.

Henceforth, we must use another approach – recognise that we can multiply any degree 2 polynomial with another degree 2 polynomial (in this case, itself) in 5 multiplications. Hence, we can use substitution to do the following:

$$Let\ y = x^{100}$$

$$Then: P(y) = A_0 + A_1y + A_2y^2$$

When we square this, we have a resultant polynomial of degree 4 and we can then uniquely determine its values at 5 points. For this, we can choose {-2, -1, 0, 1, 2} or alternatively, the 5th roots of unity. We evaluate P at these 5 points and as these are only multiplications of a large number or a scalar, the operations involved are quite cheap.

$$P(-2) = A_0 + A_1(-2) + A_2(-2)^2 = A_0 + A_1(-2) + A_2(4)$$

$$P(-1) = A_0 + A_1(-1) + A_2(-1)^2 = A_0 + A_1(-1) + A_2$$

$$P(0) = A_0 + A_1(0) + A_2(0)^2 = A_0$$

$$P(1) = A_0 + A_1(1) + A_2(1)^2 = A_0 + A_1 + A_2$$

$$P(2) = A_0 + A_1(2) + A_2(2)^2 = A_0 + A_1(2) + A_2(4)$$

By squaring these equations pointwise, we will require 5 multiplications.

$$P_b(-2) = [A_0 + A_1(-2) + A_2(4)] * [A_0 + A_1(-2) + A_2(4)]$$

$$P_b(-1) = [A_0 + A_1(-1) + A_2] * [A_0 + A_1(-1) + A_2]$$

$$P_b(0) = A_0 * A_0$$

$$P_b(1) = [A_0 + A_1 + A_2] * [A_0 + A_1 + A_2]$$

$$P_b(2) = [A_0 + A_1(2) + A_2(4)] * [A_0 + A_1(2) + A_2(4)]$$

We can then derive the coefficients from the above values by setting up a system of linear equations as it is in the form of Ax = b (i.e. A is a Vandermonde matrix). Note that this Vandermonde matrix is invertible and hence will result in unique solutions. This can be solved by inverting a constant matrix and then multiplying the matrix by the vector formed from the pointwise multiplications, which again only multiplies these results by scalars, to give the final polynomial, where we can then replace our substitute *y* with our x^{100}.

End of Solution