Yuan Gao z5239220 Q2

You are given a polynomial $P(x) = A_0 + A_1x^{100} + A_2x^{200}$ where A_0, A_1, A_2 can be arbitrarily large integers. Design an algorithm which squares $P(x)$ using only 5 large integer multiplications.

We can use the Karatsuba trick (slicing into 3 pieces):

Lets $z = x^{100}$

$P_z^2 = (A_0 + A_1z + A_2z^2)^2$

$= A_0^2 + 2A_0A_1z + (2A_0A_2 + A_1^2)z^2 + (2A_1A_2)z^3 + A_2^2z^4$

Lets:

$C_0 = A_0^2, C_1 = 2A_0A_1, C_2 = 2A_0A_2 + A_1^2, C_3 = 2A_1A_2, C_4 = A_2^2$

For $P_z = A_0 + A_1z + A_2z^2$ we have:

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

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

$P_z^2(0) = A_0^2$

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

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

Thus, if we represent the product $P_z^2 = C_0 + C_1z + C_2z^2 + C_3z^3 + C_4z^4$ we get

$C_0 = P_z^2(0)$

$$C_1 = \frac{P_z^2(-2)}{12} - \frac{2P_z^2(-1)}{3} + \frac{2P_z^2(1)}{3} - \frac{P_z^2(2)}{12}$$

$$C_2 = -\frac{P_z^2(-2)}{24} + \frac{2P_z^2(-1)}{3} - \frac{5P_z^2(0)}{4} + \frac{2P_z^2(1)}{3} - \frac{P_z^2(2)}{24}$$

$$C_3 = -\frac{P_z^2(-2)}{12} + \frac{P_z^2(-1)}{6} - \frac{P_z^2(1)}{6} + \frac{P_z^2(2)}{12}$$

$$C_4 = \frac{P_z^2(-2)}{24} - \frac{2P_z^2(-1)}{6} + \frac{5P_z^2(0)}{4} - \frac{2P_z^2(1)}{6} + \frac{P_z^2(2)}{24}$$

We can now compute

$P^2(x) = (A_0 + A_1x^{100} + A_2x^{200})^2$

Note that the expression involves only 5 multiplications:

$P_z^2(-2), P_z^2(1), P_z^2(0), P_z^2(1), P_z^2(2)$