HOMEWORK 2 – Q2

MINGLANG XIE

z5228006

2. You are given a polynomial $P(x) = A_0 + A_1 x^{100} + A_2 x^{200}$ 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. (15 pts)

Solution:

Let $y = x^{100}$

$$\begin{aligned}
\big(P(y)\big)^2 &= (A_0 + A_1 y + A_2 y^2)^2 \\
&= A_0A_0 + A_0A_1y + A_0A_2y^2 + A_0A_1y + A_1A_1y^2 + \\
&A_1A_2y^3 + A_0A_2y^2 + A_1A_2y^3 + A_2A_2y^4 \\
&= A_0A_0 + 2A_0A_1y + 2A_0A_2y^2 + A_1A_1y^2 + 2A_1A_2y^3 \\
&\quad + A_2A_2y^4 \\
&= A_0A_0 + 2A_0A_1y + (A_0A_2 + A_0A_2 + A_1A_1)y^2 \\
&\quad + 2A_1A_2y^3 + A_2A_2y^4 \\
&= A_0A_0 + (A_0A_1 + A_0A_1)y \\
&\quad + \big((A_0{+}A_0 + A_1)(A_2 + A_1) - A_0A_1 - A_0A_1 \\
&\quad - A_1A_2\big)y^2 + (A_1A_2 + A_1A_2)y^3 + A_2A_2y^4
\end{aligned}$$

Note that the last expression involves only five multiplication: $A_0A_0, A_0A_1, A_1A_2, A_2A_2$ *and* $(A_0{+}A_0 + A_1)(A_2 + A_1)$.