ASSIGNMENT2 QUESTION2

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)

Answer:

We can substitution that y = x^{100} So the $P(y) = A_0 + A_1 y + A_2 y^2$,

$$\big(P(y)\big)^2 = A_2^2 y^4 + A_1^2 y^2 + A_0^2 + 2A_2 A_1 y^3 + 2A_2 A_0 y^2 + 2A_1 A_0 y$$

Then we substitute back y with x^{100}

$$\big(P(x)\big)^2 = A_2^2 x^{400} + A_1^2 x^{200} + A_0^2 + 2A_2 A_1 x^{300} + 2A_2 A_0 x^{200} + 2A_1 A_0 x^{100}$$

$$\big(P(x)\big)^2 = A_2^2 x^{400} + 2A_2 A_1 x^{300} + (A_1^2 + 2A_2 A_0)\, x^{200} + 2A_1 A_0 x^{100} + A_0^2$$

$$\big(P(x)\big)^2 = A_2^2 x^{400} + 2A_2 A_1 x^{300} + ((A_1 + A_2 + A_2)(A_1 + A_0) - A_2 A_1 - A_2 A_1 - A_1 A_0)\, x^{200} + 2A_1 A_0 x^{100} + A_0^2$$

In this way, squares P(x) using only 5 large integer multiplications which are $A_0 A_0, A_1 A_0, A_2 A_2, A_1 A_2, (A_1 + A_2 + A_2)(A_1 + A_0)$