Name: Minh Khai Tran

zID: z5168080

**Question 2:**

* Let replace in the polynomial . We get:

where can be arbitrarily large numbers.

* If we can manage to compute somehow the product polynomial

with only 5 multiplications, we can then obtain the squared

* Since the degree of is 4 we need 5 values to uniquely determine
* We choose the smallest possible 5 integer values .
* Thus, we compute:

As we see, these evaluations involve only additions because ,

* We can now obtain with only 5 multiplications of large numbers:
* Thus, the coefficient of we can obtain those by:

Simplifying the left side, we obtain

Solve this system of linear equations for we obtain:

* Note that these expressions do not involve any multiplications of TWO large numbers and thus can be done in linear time.
* At this stage, we obtain the coefficients for the polynomial by only 5 multiplications of TWO large numbers.
* After we obtain the coefficients for the polynomial , we replace back to the to get .