Mubarra Khan z5161249 Wednesday, 24 June 2020

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.

Answer:

substituting $y = x^{100}$ we get $P_A(x) = A_0 + A_1y + A_2y^2$

$P(x)^2 = (A_0 + A_1y + A_2y^2)(A_0 + A_1y + A_2y^2)$

Using the Karatsuba algorithm

$P_A(x)^2 = A_0^2 + (2A_1A_0)y + (2A_0A_2 + A_1^2)y^2 + (2A_1A_2)y^3 + A_2^2y^4$

Define

1. $B_0 = A_0^2$

2. $B_1 = 2A_1A_0$

3. $B_3 = 2A_1A_2$

4. $B_4 = A_2^2$

5. Compute $(A_0 + A_1 + A_2)^2$ using one large integer multiplication . Then compute

$B_2 = (A_0 + A_1 + A_2)^2 - B_0 - B_1 - B_3 - B_4$

We can now compute the product polynomial
$P_B(y) = B_0 + B_1y + B_2y^2 + B_3y^3 + B_4y^4$ with only five large integer multiplications .

Since the product polynomial $P_B(y)$ is of degree 4, we need five values to **uniquely determine** $P_B(y)$. Choose the smallest possible five integer values (by absolute value). Thus we compute

$$P_A(-2), P_A(-1), P_A(0), P_A(1), P_A(2)$$

For $P_A(y)$, we have

$$P_A(-2) = 4A_2 - 2A_1 + A_0$$

$$P_A(-1) = A_2 - A_1 + A_0$$

$$P_A(0) = A_0$$

$$P_A(1) = A_2 + A_1 + A_0$$

$$P_A(2) = 4A_2 + 2A_1 + A_0$$

We can now obtain

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

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

$$P_B(0) = P_A(0)P_A(0) = A_0^2$$

$$P_B(1) = P_A(1)P_A(1)$$
$$= (A_0 + A_1 + A_2)^2$$

$$P_B(2) = P_A(2)P_A(2)$$
$$= (A_0 + 2A_1 + 4A_2)^2$$

- Simplifying everything, we obtain

$$16B_4 - 8B_3 + 4B_2 - 2B_1 + B_0 = P_B(-2)$$

$$B_4 - B_3 + B_2 - B_1 + B_0 = P_B(-1)$$

$$B_0 = P_B(0)$$

$$B_4 + B_3 + B_2 + B_1 + B_0 = P_B(1)$$

$$16B_4 + 8B_3 + 4B_2 + 2B_1 + B_0 = P_B(2)$$

- Solving the system of linear equations for B_0, B_1, B_2, B_3, B_4 we obtain

$$B_0 = P_B(0)$$

$$B_1 = \frac{P_B(-2)}{12} - \frac{2P_B(-1)}{3} + \frac{2P_B(1)}{3} - \frac{P_B(2)}{12}$$

$$B_2 = -\frac{P_B(-2)}{24} + \frac{2P_B(-1)}{3} - -\frac{5P_B(0)}{4} + \frac{2P_B(1)}{3} - \frac{P_B(2)}{24}$$

$$B_3 = -\frac{P_B(-2)}{12} + \frac{P_B(-1)}{6} + -\frac{P_B(1)}{6} - \frac{P_B(2)}{24}$$

$$B_4 = \frac{P_B(-2)}{24} - \frac{P_B(-1)}{6} + \frac{P_B(0)}{4} - \frac{P_B(1)}{6} + \frac{P_B(2)}{24}$$

- The above expressions do not involve any multiplications of two large numbers and thus can be done in linear time.

- We can now form the polynomial

$$P_B(y) = B_0 + B_1 y + B_2 y^2 + B_3 y^3 + B_4 y^4$$

We can now compute $P_B(x)^2$ in linear time via back substitution $y = x^{100}$ to get $P_B(x)^2$ as a variable of x.

Thus we have obtained $P(x)^2$ with only five multiplications.