COMP3121 Homework Q2

Arth Sanskar Patel
z5228942

June 28, 2020

1 Answer

Here we have $P(x) = A_0 + A_1x^100 + A_2x^200$. We have to square this using only 5 large number multiplications. Let $x^100 = y$, therefore we have,

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

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

$$(P(y))^2 = (A_0)^2 + (A_0A_1 + A_0A_1)y + (A_2A_0 + A_1A_1 + A_2A_0)y^2 + (A_2A_1 + A_2A_1)y^3 + (A_2)^2y^4$$

$$(P(y))^2 = A_0^2 + 2A_0A_1y + (A_1^2 + 2A_2A_0)y^2 + 2A_2A_1y^3 + A_2^2y^4$$

Here, let $F(y) = (P(y))^2$ therefore we have

$$F(y) = C_0 + C_1y + C_2y^2 + C_3y^3 + C_4y^4$$

Where,

$$C_0 = A_0^2$$

$$C_1 = 2A_0A_1$$

$$C_2 = A_1^2 + 2A_2A_0$$

$$C_3 = 2A_2A_1$$

$$C_4 = A_2^2$$

Now lets evaluate $P(y)$ at 5 smallest possible integers i.e -2,-1,0,1,2. This gives us

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

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

$$P(0) = A_0$$

$$P(1) = A_2A_1 + A_0$$

$$P(2) = 4A_22A_1 + A_0$$

Now since $F(y) = (P(y))^2$,

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

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

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

$$F(1) = (A_2A_1 + A_0)(A_2A_1 + A_0)$$

$$F(2) = (4A_22A_1 + A_0)(4A_22A_1 + A_0)$$

The 5 large multiplications above are the only multiplications so far that we need for finding the square. Replacing y for -2,-1,0,1,2 in $F(y)$ we get,

$$F(-2) = 16C_4 - 8C_3 + 4C_2 - 2C_1 + C_0$$

$$F(-1) = C_4 - C_3 + C_2 - C_1 + C_0$$

$$F(0) = C_0$$

$$F(1) = C_4 + C_3 + C_2 + C_1 + C_0$$

$$F(2) = 16C_4 + 8C_3 + 4C_2 + 2C_1 + C_0$$

Now solving the linear equations for C_0, C_1, C_2, C_3, C_4, we get

$$C_0 = F(0)$$

$$C_1 = F(-2)/12 + 2F(-1)/3 + 2F(1)/3 - F(2)/12$$

$$C_2 = -F(-2)/24 + 2F(-1)/3 - 5F(0)/4 + 2F(1)/3 - F(2)/24$$

$$C_3 = -F(-2)/12 + F(-1)/6 - F(1)/6 + F(2)/12$$

$$C_4 = F(-2)/24 - F(-1)/6 + F(0)/4 - F(1)/6 + F(2)/24$$

Solving these don't involve any large integer multiplication and can be done in linear time. With the coefficients of $F(y)$ obtained, we can put them to form the square of $P(y)$. Further more we can substitute $y = x^{100}$ to get the polynomial

$$F(x) = (P(x))^2 = C_0 + C_1x^{100} + C_2x^{200} + C_3x^{300} + C_4x^{400}$$

Reference for the answer above was taken from lecture slides of Karatsuba Algorithm.