Divide & Conquer

0. Binary Search
1. Merge Sort
2. Karatsuma's Alg for integer multiplication.

Integer Multiplication

Long multiplication: $N_1 \times N_2$

$n = n_1 + n_2$

n_1 = num digits in N_1

n_2 = num digits in N_2

$n_2 \times n_1$

- Each mult of digit x digit is $O(1)$, inclusive of adding in the old carry, recording the new carry.
- Time to write the "0"s is $O(n^2)$
- for each of the digits in N_1, multiply it by n_2 digits in N_2.
  $\therefore O(n_1 \times n_2)$ or $O(n^2)$ if $n_1 \in \Theta(n^2)$
- In worst case, $n_1 \approx n_2$, in which case running time is $O(n^2)$

$$\begin{array}{r} 184 \\ \times\ 139 \\ \hline 1656 \\ 5520 \\ 18400 \\ \hline 24576 \end{array}$$

Question: Why do we "analyze" as if multiplication can be done in constant time?

Big Int Multiplication: Karatsuba's Alg

m bits

x 1011 0110

y 1100 1011



$x_1 \; x_0$

$y_1 \; y_0$

$x = x_1 \cdot 2^m + x_0$

$y = y_1 \cdot 2^m + y_0$

$x_0 < 2^m$

$y_0 < 2^m$

$$xy = (x_1 2^m + x_0)(y_1 2^m + y_0)$$

$$= x_1 y_1 2^{2m} + (x_1 y_0 + x_0 y_1) 2^m + x_0 y_0$$

$$= z_2 \cdot 2^{2m} + z_1 \cdot 2^m + z_0$$

where $z_2 = x_1 \cdot y_1$ ← Do these two directly

$z_1 = x_1 \cdot y_0 + x_0 \cdot y_1$ ← Known to Charles Babbage.

$z_0 = x_0 \cdot y_0$

$z_3 = (x_1 + x_0)(y_1 + y_0)$

Now observe that, having computed z_0, z_2, z_3 using 3 mults, we can compute z_1 using only +/−

$$z_1 = x_1 y_0 + x_0 y_1$$

$$= x_1 y_0 + x_0 y_1 + x_1 y_1 + x_0 y_0 - x_1 y_1 - x_0 y_0$$

$$= (x_1 + x_0)(y_1 + y_0) - x_1 y_1 - x_0 y_0$$

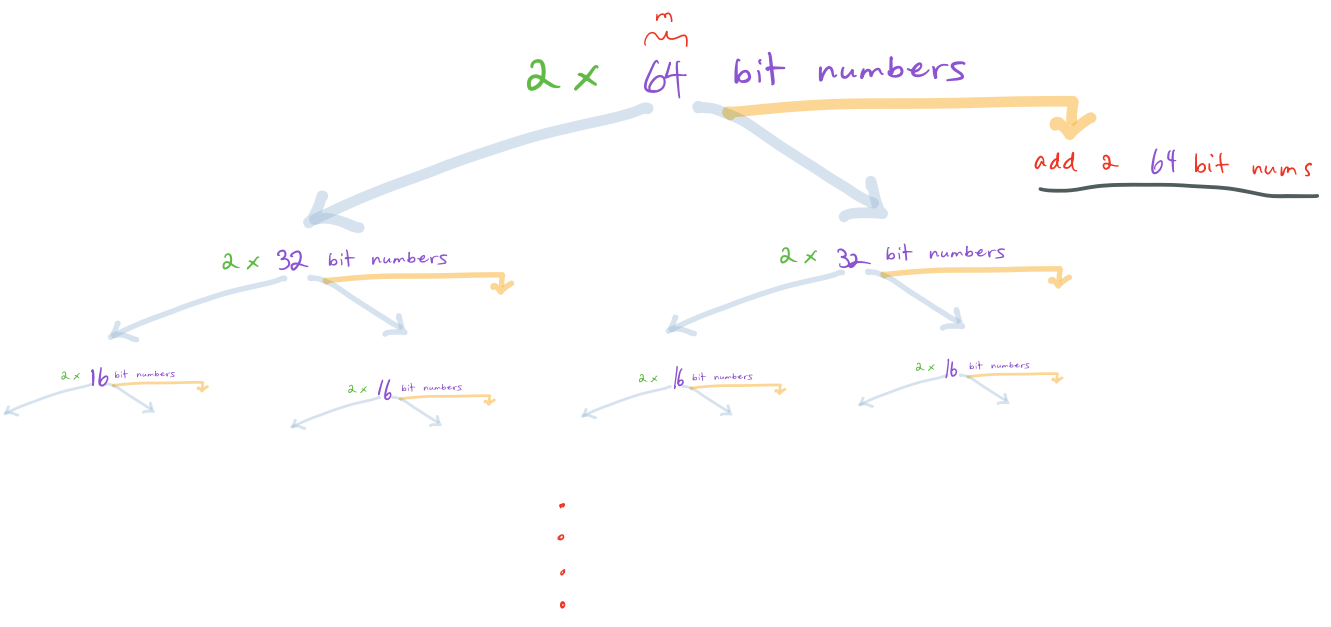
$$= z_3 - z_2 - z_0$$

(technically, z_3 computation is of m+1-bit ints, but the extra work is

Use Karatsuba recursively.

Theoretically, we could stop recursing when $m = 1$

Actually stop when ~~$2m$~~ bits is $\leq$ size of register on chip.



$$T(m) = \underbrace{3}_{a}\ T\left(\underbrace{n/2}_{b}\right) + \underbrace{n}_{f(n)}$$ ← adding 2 n-bit numbers.

$\updownarrow$

$O(n^{1.58-\varepsilon})$ ←

$n \in ?$ $\quad \Theta(n^{1.58})$

$\Omega(n^{1.58+\varepsilon})$

$\therefore$ By Master Theorem case 1,

Karatsuma's Alg runs in $\Theta(n^{\log_2 3})$