Integer Multiplication

We would like to multiply two large integers:

\[
y_{n-1}y_{n-2}y_{n-3} \ldots y_3y_2y_1y_0 \times x_{n-1}x_{n-2}x_{n-3} \ldots x_3x_2x_1x_0
\]

COMMENT: We will IGNORE carries throughout.
“Standard” Multiplication Algorithm

Elementary school algorithm with no additions until after all of the multiplies.

EXAMPLE:

\[
\begin{array}{c}
4352 \\
\times 3748 \\
\hline
16 \\
40 \\
24 \\
\hline
32 \\
08 \\
20 \\
12 \\
\hline
16 \\
14 \\
35 \\
21 \\
\hline
28 \\
06 \\
15 \\
09 \\
\hline
12
\end{array}
\]

Concatenate the “even” and “odd” indexed values within each group then sum by column.

\[
\begin{array}{c}
4352 \\
\times 3748 \\
\hline
2416 \\
3240 \\
\hline
1208 \\
1620 \\
\hline
2114 \\
2835 \\
\hline
0906 \\
1215 \\
\hline
16311296
\end{array}
\]

Atomic multiplies: \(n^2\).
Every digit on bottom is multiplied with every digit on top.

Atomic additions: \(2n(n - 1)\).
By column, right-to-left: \(0 + 2 + 4 + 6 + 8 + \ldots + 2(n - 1) + 2(n - 1) + \ldots + 8 + 6 + 4 + 2 + 0 = 2 \sum_{i=0}^{n-1} i\).
Two-digit multiplication

EXAMPLE: Base 10

\[
\begin{array}{r}
73 \\
\times 48 \\
\end{array}
\]

\[a = 4, \quad b = 8, \quad c = 7, \quad d = 3\]

\[ac = 4 \cdot 7 = 28, \quad ad = 4 \cdot 3 = 12, \quad bc = 8 \cdot 7 = 56, \quad bd = 8 \cdot 3 = 24\]

\[ad + bc = 12 + 56 = 68\]

\[2824 + 68 = 3504\]

“Every” multiplication is a two-digit multiplication ...
... with a large enough base.

EXAMPLE: Base 100

\[
\begin{array}{r}
4352 \\
\times 3748 \\
\end{array}
\]

\[a = 37, \quad b = 48, \quad c = 43, \quad d = 52\]

\[ac = 37 \cdot 43 = 1591, \quad ad = 37 \cdot 52 = 1924, \quad bc = 48 \cdot 43 = 2064, \quad bd = 48 \cdot 52 = 2496\]

\[ad + bc = 1924 + 2064 = 3988\]

\[15912496 + 3988 = 16311296\]

EXAMPLE: Base 1000

\[
\begin{array}{r}
439052 \\
\times 371448 \\
\end{array}
\]

\[a = 371, \quad b = 448, \quad c = 439, \quad d = 052\]
Recursive Multiplication Algorithm.

Use divide-and-conquer. Take two $n$ digit numbers $x, y$ and cut each in half to form:

\[
\begin{array}{c}
\begin{array}{c}
{\underbrace{y_{n-1} \cdots y_{n/2-1}}_{c}} \\
{\underbrace{y_{n/2-1} \cdots y_{0}}_{d}} \\
\end{array} \\
\begin{array}{c}
{\underbrace{x_{n-1} \cdots x_{n/2}}_{a}} \\
{\underbrace{x_{n/2-1} \cdots x_{0}}_{b}} \\
\end{array}
\end{array}
\]

\[
x = a \circ b, \quad y = c \circ d
\]

Now,

\[
xy = ac10^n + (ad + bc)10^{n/2} + bd
\]

Multiplying by a power of 10 can be accomplished by shifts (this holds for any base).

EXAMPLE:

So we need the four products $ac$, $ad$, $bc$, and $bd$, which can be attained by calling the algorithm recursively four times (on $n/2$ digit numbers). The two values $ac$ and $bd$ can be concatenated, and $ad$ can be added to $bc$ in time $\alpha n$. The final result is the sum of $ac \circ bd$ and $ad + bc$. Ignoring the rightmost $n/2$ digits of $ac \circ bd$, this sum can digit attained with and additional $\alpha n$ time plus the cost of potentially $n/2$ carries (which for simplicity we ignore). So the total time for the additions is $\alpha 2n$. The recursion ends when $n = 1$ and it multiplies two one digit numbers.

The recurrence for the time to multiply:

\[
M(n) = 4M\left(\frac{n}{2}\right) + 2\alpha n
\]

and $M(1) = \mu$. Using the tree method we find that

\[
M(n) = \mu n^2 + 2\alpha n(n - 1)
\]

This is still quadratic and matches the standard algorithm.

NOTE: In “real life” you would not recurse down to one digit, but down to the word size where the computer can do an atomic multiplication. (This comment holds for additions as well.) You can think of this as doing arithmetic in base $2^w$, where $w$ is the word size.
Returning to two-digit multiplication.

Standard Algorithm. EXAMPLE:

\[
\begin{array}{c}
52 \\
\times 36 \\
\end{array}
\]

\[
\begin{array}{c}
12 \\
30 \\
06 \\
\hline
15 \\
1872
\end{array}
\]

Four atomic multiplications and four atomic additions.

Clever Algorithm.

Two two-digit numbers can be multiplied using only \textit{three} atomic multiplications!!!

\[
cd \\
\times \ ab
\]

Form

\[
\begin{align*}
  w &= (a + b)(c + d) \\
  u &= ac \\
  v &= bd
\end{align*}
\]

Note that

\[
w = (a + b)(c + d) = ac + ad + bc + bd = ac + (ad + bc) + bd
\]

So

\[
w - (u+v) = [ac + (ad + bc) + bd] - [ac + bd] = ad + bc
\]

Just what we want!!!

The full product is

\[
xy = u10^2 + (w - (u+v))10 + v
\]

EXAMPLE:

\[
\begin{align*}
  w &= (a + b)(c + d) = (3 + 6)(5 + 2) = 9 \cdot 7 = 63 \\
  u &= ac = 3 \cdot 5 = 15 \\
  v &= bd = 6 \cdot 2 = 12
\end{align*}
\]

\[
xy = u10^2 + (w - (u+v))10 + v = 15 \cdot 100 + (63 - (15 + 12))10 + 12 = 15 \cdot 100 + 36 \cdot 10 + 12 = 1872
\]

\[
\begin{array}{c}
52 \\
\times 36 \\
\end{array}
\]

\[
\begin{array}{c}
12 \\
36 \\
\hline
15
\end{array}
\]

We have reduced the number of atomic multiplies from four to three, at the cost of increasing the number of atomic additions from four to eight.
Putting it all together

Recall

\[ w = (a + b)(c + d) \]
\[ u = ac \]
\[ v = bd \]

Then the product is

\[ xy = u10^n + (w - (u + v))10^{n/2} + v \]

EXAMPLE for four digit numbers.

\[
\begin{array}{c}
4352 \\
\times 3748 \\
\hline
\end{array}
\]

\[ w = (a + b)(c + d) = (37 + 48)(43 + 52) = 85 \cdot 95 = 8075 \]
\[ u = ac = 37 \cdot 43 = 1591, \]
\[ v = bd = 48 \cdot 52 = 2496, \]
\[ u + v = ac + bd = 1591 + 2496 = 4087 \]
\[ w - (u + v) = ad + bc = 8075 - 4087 = 3988 \]

Now it is the same as the previous example.

We can estimate the addition time as \(\alpha n/2\) to form \(a + b\), \(\alpha n/2\) to form \(c + d\), \(\alpha n\) to form \(u + v\), \(\alpha n\) to subtract that sum from \(w\), and \(\alpha n\) to add that to \(u \circ v\). The total is \(4\alpha n\). The recurrence for the time to multiply:

\[ M(n) = 3M\left(\frac{n}{2}\right) + 4\alpha n \]

and \(M(1) = \mu\). Using the tree method we find that

\[ M(n) = (\mu + 8\alpha)n^{\log_3 8} - 8\alpha n \]