Rough Idea

We can represent integers as polynomials:

$$P(z) = \sum_{i=0}^{n-1} p_i z^i$$

$$Q(z) = \sum_{i=0}^{n-1} q_i z^i$$

The integers are $P(B), Q(B)$ where B is the base (typically $B = 10$). The length of $P(B), Q(B)$ is n digits.

We want the product $R(z) = P(z)Q(z)$ specifically $R(B)$. Note that a polynomial is defined fully by its output on n points, so we can construct $R(z)$ if we have it on $2n$ points.

Evaluate it at complex roots of unity, i.e. $e^{\frac{2j\pi k}{2n}}$.

Turns out that this makes the multiplication $n \log n$ yay!!

Discrete Fourier transform:

Takes in a vector $(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{C}^n$ and outputs a vector X with

$$X[k] = (w_k|x) = \sum_{i=0}^{n-1} x[i] e^{-j\frac{2\pi}{n}ik}$$

FFT

DFT can be computed in $O(n \log n)$ time (much better than the naive $O(n^2)$ algorithm). This is because of the following remarkable fact:

Let $x[i]$ be a signal of length $2n$.

Let

$$x_e[i] = x[2i] \quad i = 0, 1, \ldots, n-1.$$

Let

$$x_o[i] = x[2i+1] \quad i = 0, 1, \ldots, n-1.$$

Observe the following about the DFT of $x[i]$.

$$X[k] = \sum_{i=0}^{2n-1} x[i] e^{-j\frac{2\pi}{2n}ik}.$$

$$X[k] = \sum_{i=0}^{n-1} x_e[i] e^{-j\frac{2\pi}{2n}2ik} + x_o[i] e^{-j\frac{2\pi}{2n}(2i+1)k}.$$

$$X[k] = \sum_{i=0}^{n-1} x_e[i] e^{-j\frac{2\pi}{n}ik} + e^{-j\frac{\pi}{n}k} \sum_{i=0}^{n-1} x_o[i] e^{-j\frac{2\pi}{n}ik}.$$

This is great, because we reduced the problem of finding the DFT of a length n signal to computing the DFT of 2 length $n/2$ signals (and then adding them with a weight on the odd DFT). There are more optimizations that go into the FFT that I haven't discussed here, but this is the gist of it. Note that if the sequence is of length $n = 2^c$ then we can just keep recursing, hence the $n \log n$ runtime.

Using this for the Integer multiplication problem

Now note that if we have the sequence $(p_0, p_1, \ldots, p_{n-1})$ of the coefficients of P, then we can compute all the terms $P(e^{j\frac{2\pi k}{2n}})$ via FFT, because

$$P(e^{j\frac{2\pi k}{2n}}) = \sum_{i=0}^{n-1} p_i (e^{j\frac{2\pi k}{2n}})^i$$