3 Mar 2021 Multiplication (§5.5)

Announcements.

1. Wellness days Tue–Wed next week.
   - no class Wed. 3/10.
   - Problem Set 4 will have only one problem.
2. Extra office hours coming this week.
   - Prof. Kleinberg Fri. 11–12
   - Watch pinned Ed post for more.

Divide and Conquer, as an alg design principle, is widely used in:

1. Processing ordered data (e.g. sorting)
2. Algebra / Arithmetic
3. Geometry

Multiplying integers.

(versions of this in ancient Greece.)

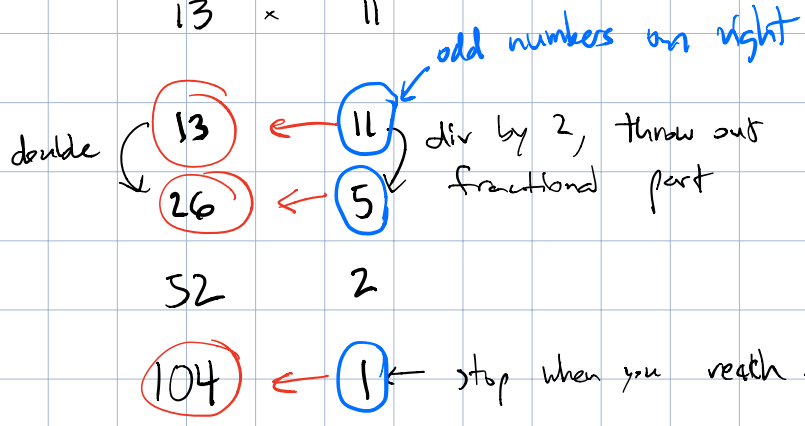
```
   13
  ×11
  ---
   13
  11
  ---
  143
```

n partial products each with n digits

To multiply two n-digit numbers this way takes $O(n^2)$.

Ethiopian multiplication.

13 × 11



Sum up circled numbers on left: $13+26+104 = 143$.

For n-digit numbers this is also quadratic.

Number of rows in table $= O(\log N)$

where $M \times N$ is the multiplication problem.

digits in $N = n = O(\log N)$.

Table has $O(n)$ rows.

Adding a subset of rows, each containing an n-digit number: $O(n^2)$.

1101 ← 13 in binary

1011 ← 11 in binary

13 → 1101

26 → 11010

0 → 000000

104 → 1101000

Karatsuba's multiplication algorithm (1800's?)

Idea: A number in base 2 is just a polynomial with $\{0,1\}$ coefficients evaluated at $x=2$.

So design a faster algorithm for multiplying polynomials!

Identity:

$$(ax+b)\cdot(cx+d) = acx^2 + (ad+bc)x + bd$$

Given coeffs a, b, c, d

We can find all coeffs of $(ax+b)(cx+d)$ using **4** multiplications and **1** addition.

Alternative: Compute

1. $e = a\cdot c$
2. $f = b\cdot d$
3. $g = (a+b)(c+d)$

$ac+ad+bc+bd$

Then the coefficients of $(ax+b)(cx+d)$ are e, $g-e-f$, f. i.e.

$$(ax+b)(cx+d) = ex^2 + (g-e-f)x + f$$

$g-e-f = \cancel{ac}+ad+bc+\cancel{bd} - \cancel{ac} - \cancel{bd}$

Conclusion: Can multiply degree-1 polynomials using 3 multiplications, 2 additions, 2 subtractions.

To multiply high-degree polynomials, use divide-and-conquer with Karatsuba's identity.

$$P(x) = p_{2n-1}x^{2n-1} + p_{2n-2}x^{2n-2} + \dots + p_1 x + p_0$$

$$= P_1(x)x^n + P_0(x)$$

degree $< n$.

$$Q(x) = q_{2n-1}x^{2n-1} + q_{2n-2}x^{2n-2} + \dots + q_1 x + q_0$$

$$= Q_1(x)x^n + Q_0(x)$$

Example: $P(x) = 4x^3 - x^2 + 2x - 6 = P_1(x)x^2 + P_0(x)$

$Q(x) = -5x^3 + 2x^2 + 7x - 3 = Q_1(x)x^2 + Q_0(x)$

$P_1(x) = 4x - 1 \qquad P_0(x) = 2x - 6$

$Q_1(x) = -5x + 2 \qquad Q_0(x) = 7x - 3$

Similar to Karatsuba we want to compute

$$[P_1(x)x^n + P_0(x)] \cdot [Q_1(x)x^n + Q_0(x)]$$

Plan: Compute $E(x) = P_1(x)\,Q_1(x)$

$F(x) = P_0(x)\,Q_0(x)$

$G(x) = (P_1(x)+P_0(x))(Q_1(x)+Q_0(x))$

Use

$$P(x)\cdot Q(x) = E(x)x^{2n} + \underbrace{(G(x)-E(x)-F(x))}_{\text{degree} < 2n}x^n + F(x)$$

Conclusion. To multiply polynomials of degree $< 2n$ we need to do

- 3 mult. of poly degree $< n$.
- 2 add. — — — $< n$.
- 2 sub. — — — $< 2n$

Ordinarily in a quad time alg, doubling the input size quadruples amt of work. But doubling polynomial degree only triples the amount of multiplications

$\Longrightarrow$ we should be able to beat $O(n^2)$.

How to analyze # of arithmetic operations?

Let $A(n)$ denote # arith ops performed when using Karatsuba's to multiply polynomials of degree $< n$.

$$A(2n) = 3A(n) + 6n.$$

Solving the recurrence by "unrolling" it:

$$A(n) = 3A\left(\tfrac{n}{2}\right) + 3n$$

$$= 3\left[3A\left(\tfrac{n}{4}\right) + 3\left(\tfrac{n}{2}\right)\right] + 3n$$

$$= 9A\left(\tfrac{n}{4}\right) + \tfrac{9}{2}n + 3n$$

$$= 27A\left(\tfrac{n}{8}\right) + \tfrac{27}{4}n + \tfrac{9}{2}n + 3n$$

$$= \ddots$$

after $\log(n)$ iterations: $\log(n)$ denotes $\log_2(n)$.

$$= 3^{\log(n)} \cdot \underbrace{A(1)}_{1} + 3n \cdot \left(\sum_{k=0}^{\log_2(n)-1} (3/2)^k\right)$$

$$= 2^{\log(3)\cdot\log(n)} \cdot 1 + 3n\left(\frac{(3/2)^{\log n} - 1}{3/2 - 1}\right)$$

$$= \left[2^{\log(n)}\right]^{\log 3} + 3\cdot 2\cdot\left(2^{\log n}\right)\cdot\left(\left(\tfrac{3}{2}\right)^{\log n} - 1\right)$$

$$= n^{\log 3} + 6\cdot\left(3^{\log(n)} - 2^{\log n}\right)$$

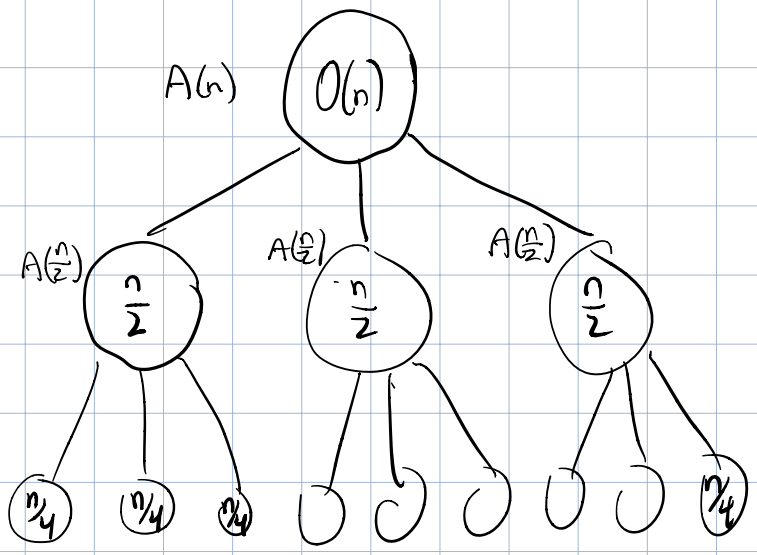
$= 7 \cdot n^{\log 3} - 6n.$

$\log(3) \approx 1.58$

Time complexity $O(n^{1.58})$ rather than $O(n^2)$.

Diagrammatic method for solving

$$A(n) = 3A(\tfrac{n}{2}) + O(n).$$



← Level 0

← Level 1

Tree has $\log_2(n)$ levels.

Total work at level 0: $O(n)$

Level 1: $O(3n/2)$

Level 2: $O(9n/4)$

$\vdots$

level k: $O\left(\left(\frac{3}{2}\right)^k \cdot n\right)$.

Combined we have

$$n \cdot \boxed{\sum_{k=0}^{\log(n)-1} (3/2)^k}$$ ← A geometric sum is $O(\text{largest term})$.

$$= O\left(n \cdot (3/2)^{\log(n)-1}\right)$$

$$= O\left(2^{\log n} \cdot (3/2)^{\log n} \cdot 2/3\right)$$

$$= O(3^{\log n}) = O(n^{\log 3}).$$

Faster still: memorize the "Master Theorem" for solving recurrences.