Introduction to Cryptography

Computational complexity

PCMI 2022 - Undergraduate Summer School

We will be talking about algorithms

specific "recipe" to do something

"exponentiation" is not an algorithm

compute g^3 :

· g^2

· $g^2 \cdot g$

vs fast modular exponentiation

We will want to talk about the <u>computational complexity</u> of a given algorithm

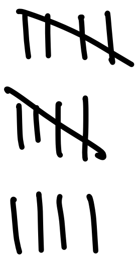
This is roughly the amount of <u>resources</u> needed to do the computation

time, number of arithmetic steps

space or memory

We will talk about "schoolbook multiplication"

$$\begin{array}{r} 1 \\ 125 \\ \cdot\ \ 213 \\ 1 \\ \hline *\ 375 \\ 1250 \\ 25000 \\ \hline 25 \end{array}$$



steps: single digit

+ OR ×

Karatsuba

Toom-Cook

fastest alg due in part Harvey

The exact number of steps when multiplying 2 3-digit numbers depends on the digits because of the carries

2 3-digit #s

But most of the operations when multiplying are multiplications

single-digit mult.

Number of steps to multiply 2 5-digit numbers

as few as 41

as many as 74

33

Number of steps to multiply 2 k-digit numbers

as few as $2k^2 - 2k + 1$

as many as $3k^2 - 1$

$$2k^2-2k+1 = k^2 + \frac{k(k-1)}{2} + \frac{(k-1)(k-2)}{2}$$

$$3k^2-1 = 2k^2-2k+1 \quad + \quad k(k-1)+k+2(k-1)$$

After a while, we see that the "right" input to a function counting the number of steps is the <u>size</u> (the number of digits) of the numbers being multiplied.

$$k = \lfloor \log_{10} n \rfloor + 1$$

formula to compute the size k of the number n

$$\# \text{ of bits} = \lfloor \log_2 n \rfloor + 1$$

By abuse of the word function,

let $f(k)$ = # steps to multiply 2 k-digit numbers

for us $\quad k^2 \leq f(k) \leq 3k^2$

Definition 1

natural numbers $\mathbb{Z}_{>0}$

Let $f, g: \mathbb{N} \to \mathbb{N}$

positive real

Then $f \ll g$ is there are constants

a, b such that if $k \geq a$ then

$$f(k) \leq b g(k)$$

when the input is large enough

f is less than a constant times g.

Also $f \in O(g)$ OR $f = O(g)$

Definition 2

Let $f, g : \mathbb{N} \to \mathbb{N}$

We say $f >> g$

- if $g << f$
- equivalently if there are real constants a, b with

$$f(k) \geq b g(k) \quad \text{when} \quad k \geq a$$

Also $f \in \Omega(g)$ or $f = \Omega(g)$

Note that Ω is slightly different in analytic number theory

Definition 3

We say $f \sim g$ if $f \ll g$ and $g \ll f$

Read "f is on the order of g"

Real notation $f = \Theta(g)$ or $f \in \Theta(g)$

Proposition

If $\lim_{k \to \infty} \frac{f(k)}{g(k)}$ exists and is finite then $f \ll g$.

3 main speeds at which f can grow

① slow growth:

We say that f grows polynomially if there are positive real constants a, b with

$$k^a \ll f(k) \ll k^b$$

(Silverman said "f is quadratic means $f \sim k^2$")

② fast growth

f grows exponentially if $\exists\, a, b > 0$ and real

with

$$2^{ak} \ll f(k) \ll 2^{bk}$$

③ medium

f grows subexponentially if $\forall\, a, b > 0$ and real

with $$k^{a} \ll f(k) \ll 2^{bk}$$

That’s all for now!