

Algebra And Algorithms

- FACTORIZATION OF POLYNOMIALS
- PRIMALITY TESTING
- GRAPH ISOMORPHISM
- ~~MATRIX MULTIPLICATION~~
- Course Wrap up..



1. History: "Algebra" (Al Jabr) comes from a text by Al Khwarizmi ("Algorithm")

- Names Intertwined !!

- Remarkable Algorithms (to me most surprising) are algebraic
 - Greatest Common Divisor (Euclid)
 - Determinant (Gauss).

Aside: Determinant

(2)

- formal Definition:

$$\begin{aligned} \textcircled{1} \text{ Sign}(\pi) &= +1 \quad \text{if } \pi \in S_n \text{ is } \underline{\text{even}} \\ &= -1 \quad \text{if } \pi \in S_n \text{ is } \underline{\text{odd}} \end{aligned}$$

$$\textcircled{2} \text{ Det}(M) = \sum_{\pi \in S_n} (-1)^{\text{sign}(\pi)} \cdot \prod_{i=1}^n M_{i, \pi(i)}$$

$M \in \mathbb{F}^{n \times n}$ is $n \times n$
matrix over
field \mathbb{F} .

- Definition involves $n! \approx \binom{n}{0}^n$ summands.

- But can be computed in polynomial time.

- Contrast

$$\begin{array}{ccc} \text{Perm}(M) & = & \sum_{\pi \in S_n} \prod_{i=1}^n M_{i, \pi(i)} \\ \uparrow & & \uparrow \\ \text{for permanent} & & \text{No signs!} \end{array}$$

- Belief: Perm(M) requires $\exp(n)$ time to compute

$P \neq NP \Rightarrow$ Belief

Polynomials + Algorithms

① Addition: Takes $\Theta(n)$ time for adding two deg n polynomials

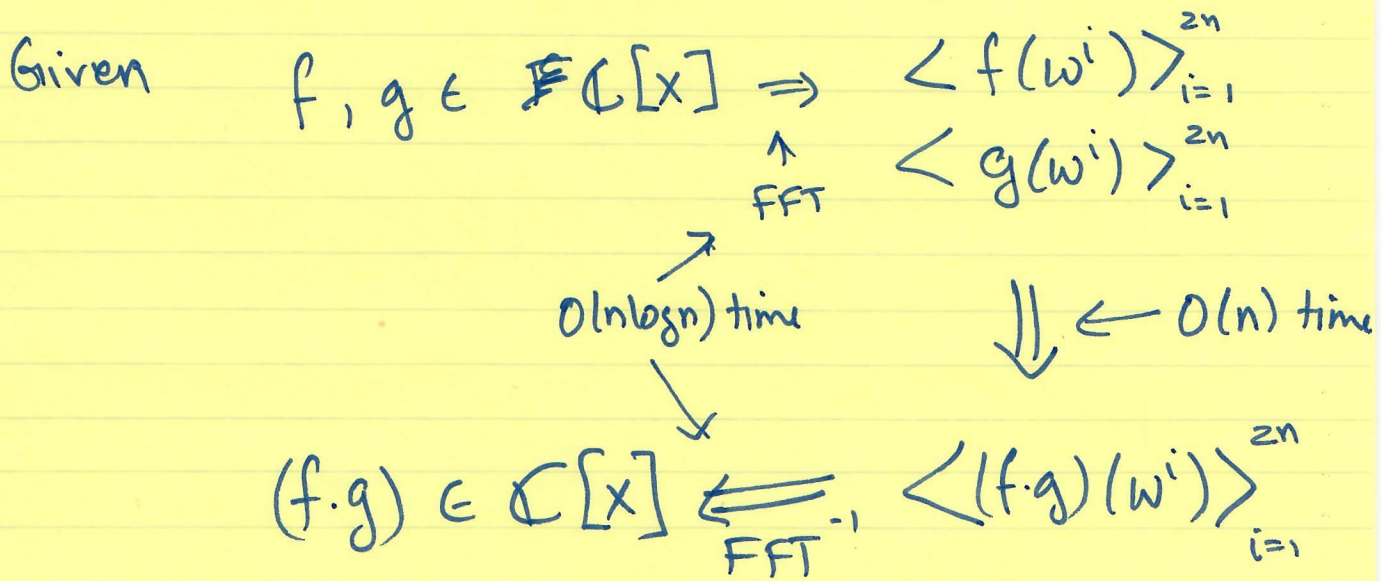
② Multiplication: Naively $O(n^2)$.

- But ~~slight~~ can do better. - Karatsuba $O(n^{1.58})$

- Even better: $O(n \log n \log \log n)$ field operations
[over any field]

Essence of idea (over \mathbb{C})

Let ω be 2^n root of unity



Polynomials + Algorithms - 2

③ Interpolation: Given $\alpha_1 \dots \alpha_n$ compute coeff. of f
 $f(\alpha_1) \dots f(\alpha_n)$ ($\deg f < n$)

$O(n \log^c n)$ for some $c \leq 3$.

④ Multipoint Evaluation: Given coeff of f & $\alpha_1 \dots \alpha_n$
 compute $f(\alpha_1), \dots, f(\alpha_n)$

$O(n \log^c n)$ for some $c \leq 3$

⑤ Division with Remainder: Given f, g compute
 q, r with $\deg r < \deg g$ s.t.

$$f(x) = q(x) \cdot g(x) + r(x)$$

$O(n \log^c n)$

⑥ GCD: $O(n \log^c n)$

⑦ FACTORIZATION: $O(n^{1.5})$ roughly.

(~~It's~~ Even polytime is non-trivial!).
 (Field specific).

FACTORIZATION OVER FINITE FIELDS

\mathbb{F}_q - field of size q

Key Idea:

$$X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha)$$

- So if $X^2 - ax + b = (X - \alpha) \cdot (X - \beta)$

then $\gcd(X^2 - ax + b, X^q - X) = X^2 - ax + b$!

- But $(X^q - X) = X(X^{\frac{q-1}{2}} - 1)(X^{\frac{q-1}{2}} + 1)$ [q odd]

- Hopefully:

$$\gcd(X^2 - ax + b, X^{\frac{q-1}{2}} - 1) \neq 1, X^2 - ax + b$$

- for typical polynomials ... w.p. $\frac{1}{2} \nmid (X - \alpha) \mid X^{\frac{q-1}{2}} - 1$
 $\frac{1}{2} \nmid (X - \beta)$ does not.

- to get all poly, factor

$$(X - \gamma)^2 + a(X - \gamma) + b \quad \text{for random } \gamma \text{ of our choice.}$$

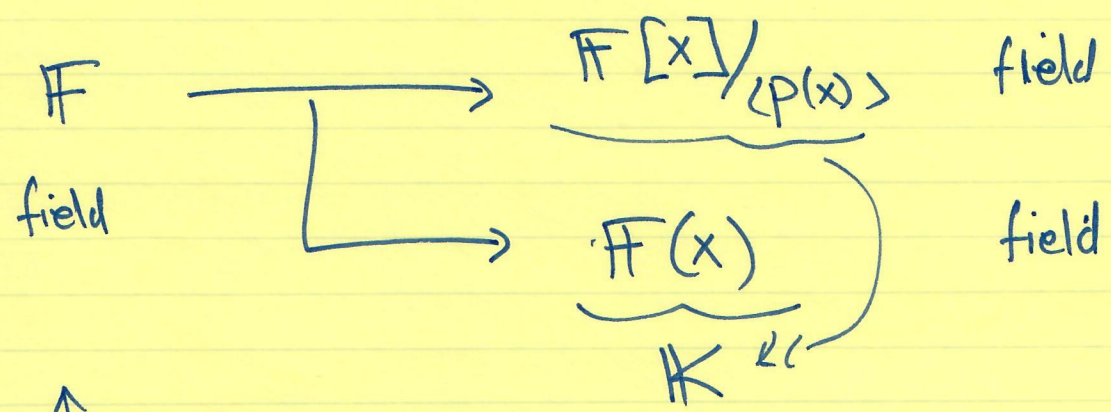
\leadsto
 $X^2 + a'X + b'$; roots $\gamma + \alpha, \gamma + \beta$

w.p. $\geq \frac{1}{2}$ $(X - (\gamma + \alpha)) \mid X^{\frac{q-1}{2}} - 1$
over r

Basis of factoring all kinds of polynomials

- Over rationals,
- Multivariate,
- Function fields.

One Key Notion



\uparrow
 Given factorization
 alg for $F[z]$

\implies

Can get factorization
 alg. for $K[z]$
 for either way
 to get K

PRIMALITY TESTING

- Given $0 \leq N \leq 2^n$, ~~compute~~ determine if N is prime.
- 70's [Rabin, Miller, Solovay-Strassen]:
 - Randomized $\text{poly}(n)$ time algorithm to test primality.
 - But no "proof" of primality

- 2003: [Agarwal, Kayal, Saxena]
 - Deterministic algorithm for primality
 - via Algebra!!

• Key Idea.

for $a \neq 0$ $(x+a)^N = x^N + a \pmod{N}$

$\Leftrightarrow N$ is prime.

8

• But how to check identity? takes $\sim N$
 $= \text{exp}(n)$ time

• Idea 1: Pick $Q(x)$ of degree $\sim (\log N)^2$
at random. Verify

$$(x+a)^N = x^N + a \pmod{N, Q(x)}$$

[Still randomized. No proofs of primality.]

• Idea 2: Pick $Q(x) = x^r - 1$ for ~~small~~
 $r \approx (\log N)^3$

Final Algorithm:

for $a = 1 \dots (\log N)^2$ do

for $r = 1 \dots (\log N)^3$ do

verify $(x^N + a) = (x+a)^N \pmod{N, x^r - 1}$

end

end

Accept if all tests accept.

• Key ingredient in analysis. $Q[x] / (N, x^r - 1)$

9

Graph Isomorphism

Given: $G = (V, E)$ $E \subseteq V \times V$

$\&$ $H = (W, F)$ $F \subseteq W \times W$

are G & H isomorphic?

i.e. $\exists \phi: V \rightarrow W$ 1-1

s.t. $(\phi(u), \phi(v)) \in F \iff (u, v) \in E$?

————— λ —————

History: Long known to be in "NP"

: Not believed to be "NP-hard"

: But no polytime algorithms known.

Best till 2015: $\sim 2^{\sqrt{n}}$

: [Babai 2015]: $O(n^{\log n})$ time algorithm.

[Not poly but almost!]

Key Idea: Solve "String Isomorphism"

String Isomorphism:

- Given $a, b \in \Sigma^n$ for finite Σ ,
- ~~s.t.~~ $\{ \pi_1, \dots, \pi_k \} \subseteq S_n$ generating group G .

- Determine if $\exists \pi \in G$ s.t.

$$a \cdot \pi = b \quad [\forall i \in n \quad a_{\pi(i)} = b_i]$$

————— x —————

* Easy: Graph Isomorphism \leq String Isomorphism.

• Hard part: String Isomorphism in time $O(n^{log n})$.

- lots of group Theory

- New Algorithms in Group Theory

[Membership in Permutation Groups
used heavily.]