How to factor objects?

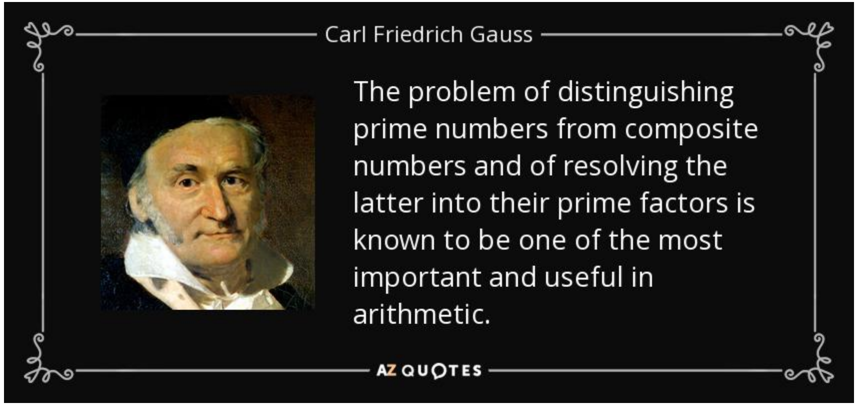
Nitin Saxena
CSE@IIITK

SWW Indore
December 2025

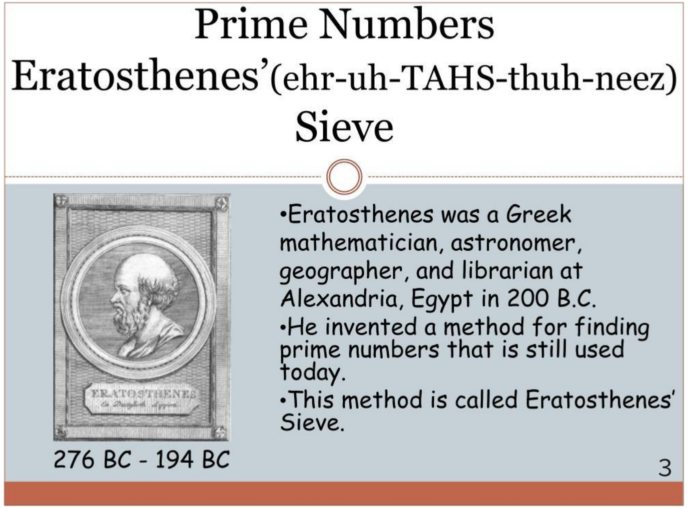
Base cases

Integers

- Integer n factors *uniquely* into prime numbers.
  - Eg. $1092 = 2^2 * 3 * 7 * 13$



- Given n, can you factor it?
  - Input n in binary
  - $2^{(\log n)^{0.3}}$ time not good enough
  - Number Field Sieve (1990s) factors via $x^2 = y^2 \bmod n$



- Hardness used in cryptosystems.
  - RSA, HTTPS, SSh, SFTP, Diffie-Hellman, Banks, Whatsapp, ...

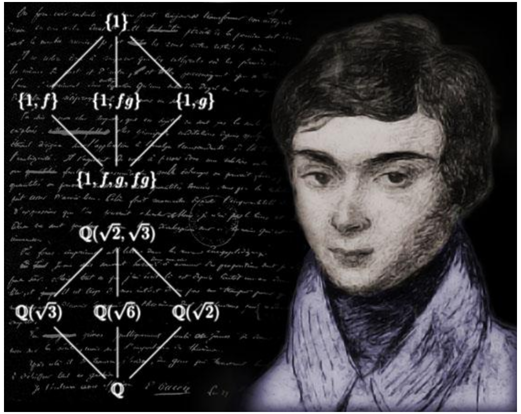
Univariate over integers

- Given polynomial $f(x) \in \mathbb{Z}[x]$, factor it.
  - $f = x^5-x^4-4x^2+x-2$ factors
  - Roots have no formula
  - Irreducibility testing?

- [Lenstra,Lenstra,Lovász'82] solved this completely.
  - Factor mod $2, 2^2, 2^4, 2^8, \ldots$
  - Lift to integral factor using lattice theory
  - Useful in many *post-quantum* cryptosystems

Univariate over finite fields

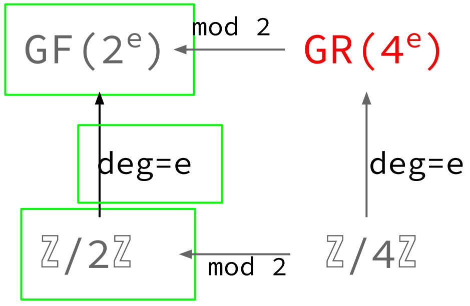
- Galois field $GF(p^e)$ of size p^e and char = prime p.
- Given polynomial $f(x) \in GF(p)[x]$, factor it.
  - $f = x^2-2$ factors mod 7
  - $\sqrt{2} = 3 \bmod 7$!
  - Irreducibility testing?



- [Berlekamp'67; Cantor-Zassenhaus'81] solved this practically.
  - Use Galois automorphism
  - Compute gcd of f(x) with x^p-x, $x^{p^2}-x$, $x^{p^3}-x$,...
  - Useful in crypto, coding theory, computational algebra, arithmetic-geometry, ...

Univariate over Galois rings

- Galois ring $GR(p^{ke})$ of size p^{ke} and characteristic = prime-power p^k.
- Given polynomial $f(x) \in GR(p^{ke})[x]$, factor it.
  - $f = x^2-2$ factors mod 7^2
  - $\sqrt{2} = 10 \bmod 7^2$!
  - Irreducibility testing?

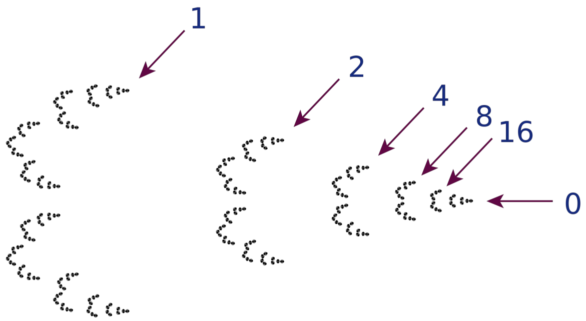


- This problem is OPEN.
- [Dwivedi,Mittal,S.'19] solved for $k=4$.
  - Factor $f(x)$ mod p, p^2, p^3, p^4.
  - Lifting from one to the next precision is *nontrivial*.
  - Eg. $f = x^2-p \bmod p^2$ vs $f = x^2-px \bmod p^2$

Univariate over p-adic numbers

- Hensel (1897) defined p-adic numbers Z_p.
  - $1+2p+3p^2+4p^3+5p^4+...$ converges to a number!
- Given polynomial $f(x) \in Z_p[x]$, factor it.
  - $f = x^2-2$ factors in 7-adic
  - $\sqrt{2} = 3 + 1*7 + 2*7^2 + 6*7^3 + ...$ in infinite digits!
  - Irreducibility testing?

- [Chistov'90; Cantor,Gordon'00] solved it efficiently.
  - Newton polytope of f(x),
  - coupled with p-adic metric,
  - reduces to mod p factoring.
  - Useful in computational number theory.

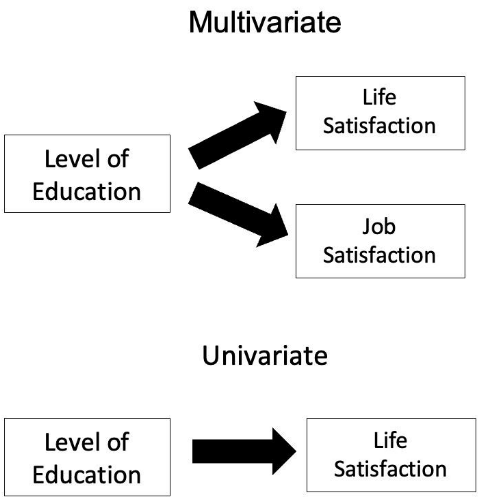


Multivariates

Multivariate sparse polynomials

- Given polynomial $f(x_1,x_2,...,x_n) \in F[\mathbf{x}]$, factor it.
  - $f = (x_1^d-1)...(x_n^d-1)$ factors into
  - $g = (x_1^{d-1}+...+x_1+1)...(x_n^{d-1}+...+x_n+1)$.
  - Sparsity $s:=2^n$ blows-up to d^n.
  - => Factors can be very large!
- What if individual-degree d is constant?

- [Bhargava,Saraf,Volkovich'18] showed a quasipoly bound.
- [Bisht,S.'22] showed a poly bound for *symmetric* factors.
  - Newton polytope of $f(\mathbf{x})$
  - Relation between #vertices & #internal points.
  - Fast algorithm, by reducing to the base cases

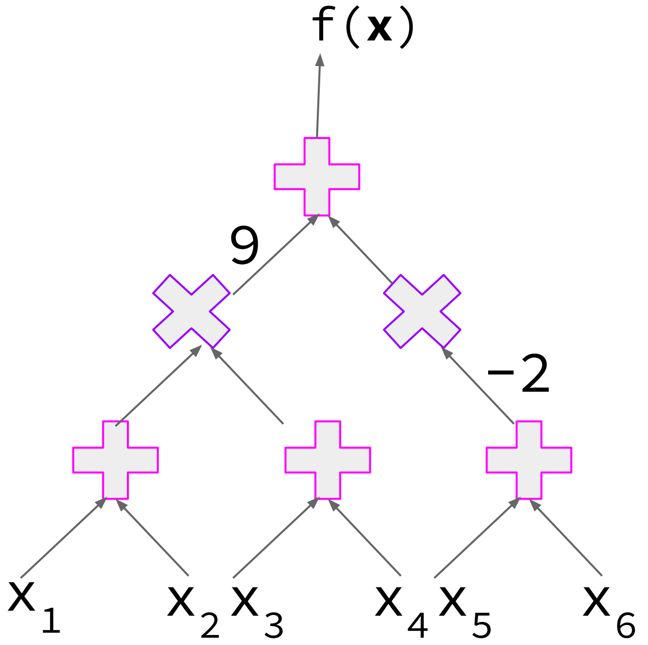


IN FORMULA MODEL

- Given polynomial $f(x_1,x_2,...,x_n) \in F[\mathbf{x}]$, factor it.
  - Input: is a formula of size s.
  - Output: is a formula of size =?

- Only quasipoly bound known till 2024.
- [BKRRSS'25] prove Poly bound in 2025.

- **Idea**: Use an expression for the roots given by Lagrange Inversion formula of analytic functions.



Lagrange Inversion Theorem.

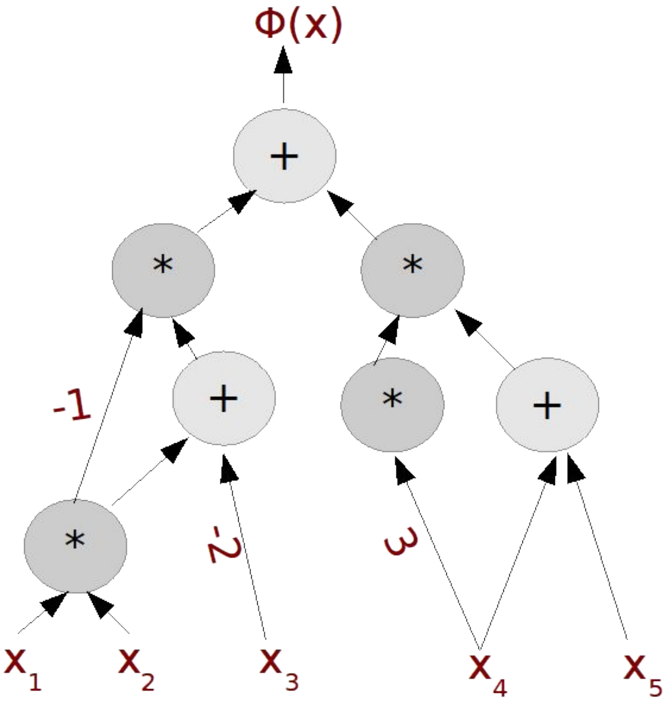
If a GF $g(z) = \sum_{n\geq 1} g_n z^n$ satisfies the equation $z = f(g(z))$ with $f(0) = 0$ and $f'(0) \neq 0$ then $g_n = \frac{1}{n}[u^{n-1}]\left(\frac{u}{f(u)}\right)^n.$

In circuit model

- Given polynomial $f(x_1,x_2,...,x_n) \in F[\mathbf{x}]$, factor it.
  - Input: is a circuit of size s.
  - Output: is a circuit of size =?

- [Kaltofen'87] showed a poly bound.
  - degree not too `high'

- **Idea**: Same as formula.
  - Works with constant-depth circuits!

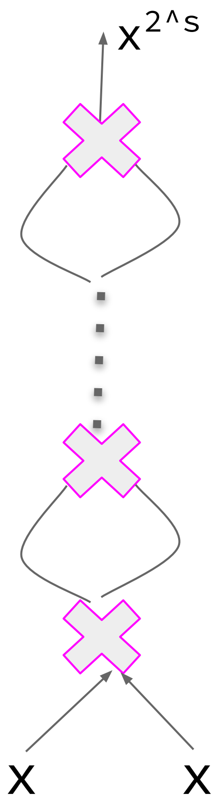


In a 'tougher' circuit model

- Given polynomial $f(x_1,x_2,...,x_n) \in F[\mathbf{x}]$, factor it.
  - Input: is a circuit of size s and degree 2^s.
  - Output: a factor of degree poly(s) of size =?

- It's an **open** question.
- [Dutta,S.,Sinhababu'18] showed a poly bound, when
  - degree of the radical of f is not too `high'.

- **Idea**: all-roots-Newton-iteration is doable inside circuits.



Conclude with open problems

- Question 1: Fast integer factoring?
- Question 2: Fast polynomial factoring mod p^k?
- Question 3: General circuit factoring?
- Question 4: Derandomization?

THANKS!

Survey @ www.cse.iitk.ac.in/users/nitin/

question