Computational Algebra & Number theory

- Computation & algebra have enriched each other. Egs.

Comp. enriching algebra

1) Euclid's gcd algorithm for integers. gcd(a, b) is a new algebraic tool.

2) Galois' attempt to find roots of a polynomial. $f(x) = x^2 + 3x + 1$.

$\Rightarrow$ Galois' solution led to the development of modern algebra.

3) <u>Weil's</u> attempt to study roots of a bivariate polynomial $f(x,y)$, over finite fields. Led to developing algebraic geometry.

Algebra enriching computation:

1) Many optimization problems reduce to <u>SAT</u>. Eg. $\phi = (x_1 \vee x_2 \vee \bar{x}_3) \wedge (\bar{x}_2 \vee x_3)$.

<u>Qn:</u> Is ϕ satisfiable?

<u>Alternative formulation:</u> poly. system over $\mathbb{F}_2 = GF(2)$

$$\begin{cases} (1-y_1)(1-y_2)y_3 = 0. \\ y_2 \cdot (1-y_3) = 0. \end{cases}$$

[over any $\mathbb{F}$?]

2) <u>Coding theory</u>:

Alice $\longrightarrow$ Bob

m $\quad C(m)$ $\qquad C(m)+E = c'$

<u>Qn</u>: How to efficiently code m & decode with errors?

[The best ways known are algebraic.]

3) Internet Security:

$$A \longrightarrow B$$

$(m \mapsto C(m))$ Intruder $(C(m) \mapsto m)$

Qn: Encryption/Decryption efficiently & high security "guarantee"?

[The best ways are algebra/number theory.]

Course Outline

- The above introduction motivates the following topics:
  - Fast algos for multiplying (or dividing) integers & polynomials.
  - Fast poly. factorization [eg. codes]
  - Lattices & short vectors [eg. NTRU crypto-system]
  - Primality testing [applied in RSA cryptosystem]

- Integer Factoring (breaking RSA!)
- Discrete logarithm. $[a^x \equiv b \bmod n]$
- Advanced topics — Elliptic Curves & Point Counting over finite fields.

- Refs. listed on the homepage/teaching.
- Grading: 24% Assgns.
  35% Midsem, Endsem each
  6% Participation/Extra Talk

- Basic Complexity Notation:

- **Algorithm**: Formally, it's a Turing machine. Informally, it's a routine implementable on any computer.
- **Asymptotics**: Obvious resources < Time / space

  We express them as a function of the input size $|x|$ (bit-size).

Polynomial-time : **P** : set of problems solvable in time $\leq |x|^c$, constant c.

Exponential-time : **EXP** : ------ time $\leq 2^{|x|^c}$.

▷ $P \subsetneq EXP$ ....

Randomized Polynomial-time : **BPP** : set of problems solvable in poly-time given unbiased coins (to toss!)

[error $\leq 1/3$]

Basic Algebra Notation:

- **Fields**: algebraic object with $+, \times$ associativity, commutative, distributive, identity ($0, 1$ resp.), inverses ($-a, \frac{1}{a}$).

egs: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{C}(x_1) := \left\{ \frac{f(x_1)}{g(x_1)} \mid f, g \in \mathbb{C}[x_1] \right\}$

$\mathbb{Q}$: discrete; $\mathbb{R}$: continuous; $\mathbb{C}$: alg. closed

$\rightarrow$ char $= 0$ fields

- char $= p$ (prime) [?. Exercise]

- Exercise: $\mathbb{Z}/\langle n\rangle$ is a field $\Longleftrightarrow$ n is prime
(integers mod n)

- Eg. $n=6$, • 2^{-1} mod 6 undefined.
• $2\times 3\equiv 0$ mod 6

Exercise: 1) Finite field has size $=$ p-power.
2) $\exists$ unique field of size p^d.
(denoted by $\mathbb{F}_{p^d}$)

Rings are like fields except we drop commutativity & inverse (on $\times$).

- Eg. $\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{H}(\mathbb{Q})$, $M_n(\mathbb{Q})$

domain

polynomial ring

quaternions

$n \times n$ matrices over $\mathbb{Q}$

Ideals I of ring R with $(+, \times)$ & $R \cdot I \subseteq I$.

Exercise: $R/I := (\{r + I \mid r \in R\}, +, \times)$ is a ring!

$(R \bmod I)$

- Morphisms : homomorphism, isomorphism, automorphism, epimorphism, monomorphism, endomorphism.

$$\phi : (R_1, +, \times) \longrightarrow (R_2, +, \times)$$
$$a \longmapsto \phi(a)$$
$$b \longmapsto \phi(b)$$
$$a+b \longmapsto \phi(a)+\phi(b)$$
$$a \times b \longmapsto \phi(a) \times \phi(b)$$

<u>Groups</u> are objects with a single operation $\times$ (& natural properties):
(abelian?)

e.g. $(\mathbb{F}, +)$, $(\mathbb{F}^* := \mathbb{F}\setminus\{0\}, \times)$,
$(GL_n(\mathbb{F}), \times)$,
$\mathbb{F} \in$ field.
invertible matrices $n\times n$

<u>Exercise:</u> $(\mathbb{F}_{p^d}^*, \times)$ is cyclic group.

- $(G, *)$ is <u>cyclic</u> if $\exists\, g \in G$ s.t. $\{g, g^{-1}\}$ together generate G using $*$.
generator

- Eg. 1: $(\mathbb{Z}, +)$ is cyclic group with generator 1.

$\langle -1, 1 \rangle_{+} = (\mathbb{Z}, +)$

- Eg. 2: $(\mathbb{Z}/n\mathbb{Z}, +)$ "

$\langle 1 \rangle = (\mathbb{Z}/n\mathbb{Z}, +)$

<u>Exercises:</u> 1) Any ∞ cyclic group is isomorphic to $(\mathbb{Z}, +)$.

2) Any size-n cyclic group " " to $(\mathbb{Z}/n\mathbb{Z}, +)$.

Asymptotics

- Let $f, g : \mathbb{N} \longrightarrow \mathbb{R}^+$. The comparisons are:

upper bound / lower bound

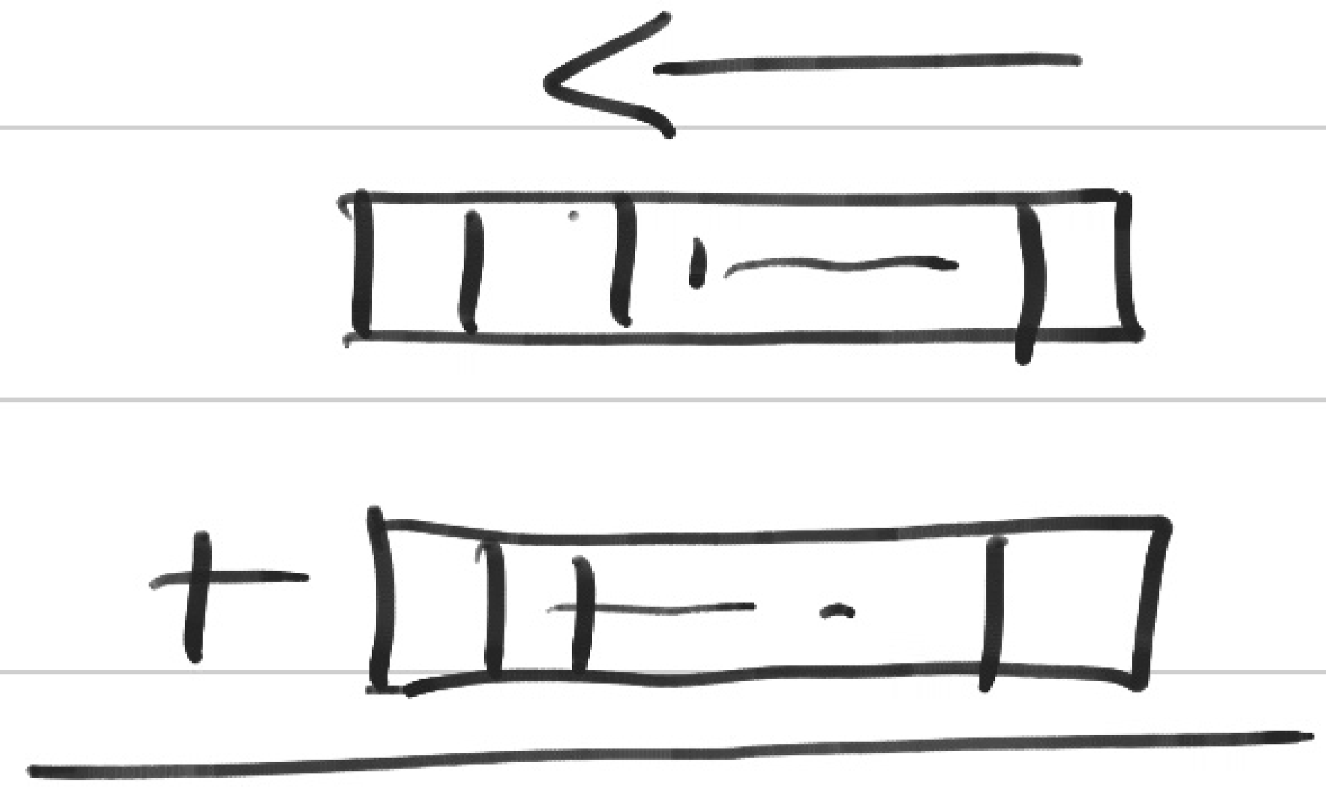
$f(n) = O(g(n))$, $g(n) = \Omega(f(n))$

$f = o(g)$, $g = \omega(f)$

$f = \Theta(g)$

$f = \tilde{O}(g)$: $f = O(g \cdot (\log g)^c)$ for constant c.

4. Easy arithmetic in $\mathbb{Z}$



1) $a \pm b$ in

$O(\lg|a| + \lg|b|)$ – bit operations.
(time)

2) $a \times b$ in

$O(\lg|a| \cdot \lg|b|)$ – time.

3) q & r s.t. $a = q \cdot b + r$ $(0 \leq r < b)$

in $O(\lg|q| \cdot \lg|b|)$ – time.