A “gentle” introduction to Computational Number Theory

CNT@SSHS #002

05/01/2019 (Wed)

4411 윤창기

Contents

- Computational Complexity and Input size

- Toy problem : Determinant of an integer matrix
  - Chinese Remainder Theorem over $\mathbb{Z}/p\mathbb{Z}$

- Hold up.
  - Is $\mathbb{Z}/p\mathbb{Z}$ the “fundamental basis” for CRT? : Rings and Ideals

Complexity & Input Size

$T(n) = O(f(n))$.

What the heck is “n”???

Complexity

Problem.

Sort the n integers in the input in non-decreasing order.

Complexity

Problem.

Sort the n integers in the input in non-decreasing order.

Complexity.

Time Complexity : $O(n \lg n)$

Space Complexity : $O(n)$

What is “n”?? : # of integers in the input!!

Sorting algorithm has *a linearithmic complexity* for n.

Com..plex..ity..?

Problem.

Sort the 2^n integers in the input in non-decreasing order.

Complexity.

Time Complexity : $O(2^n \lg 2^n) = O(n2^n)$

Space Complexity : $O(2^n)$

Sorting algorithm has *an exponential complexity* for n???

Now, what is the meaning of “n”??

A “trivial” premise

The “scale of complexity” should be determined with the “amount of input”.

$$T_{\text{sort}}(\#) = O(\# lg \#)$$

Discrete Logarithm Problem

Problem.

Given a, p and g (a primitive root of p), acquire the minimal $k \geq 0$ satisfies $g^k \equiv a \pmod{p}$.

Complexity.

With Baby - step Giant - step,

Time Complexity : $O(\sqrt{p})$.

Space Complexity : $O(\sqrt{p})$.

Discrete logarithm can be found in *sublinear complexity?*

Discrete Logarithm Problem

Problem.

Given a, p and g (a primitive root of p), acquire the minimal $k \geq 0$ satisfies $g^k \equiv a \pmod{p}$.

Complexity.

With Baby - step Giant - step,

Time Complexity : $O(\sqrt{p})$.

Space Complexity : $O(\sqrt{p})$.

NoPe

Discrete logarithm can be found in *sublinear complexity?*

Scale of BsGs

The “scale of complexity” should be determined with the “amount of input”.

Amount of input：$\boldsymbol{O(\lg p)}$

Complexity：$O(\sqrt{p} = 2^{\frac{\lg p}{2}})$

Input length

Input length := “Minimal # of bits to represent the input”.

The algorithm works in **polynomial complexity**, if there exists a const. c s.t. $T(n) = O(n^c)$.

- A firm definition of time complexity

Our PoV

- We only focus on the “polynomiality” of an algorithm, not the exact complexity.

- If an algorithm on n integers works in $O\big((n \log p)^c\big)$ time, everything is good :)

TMI : P vs NP

- P : Set of **decision problems**, solvable in polytime
  with a deterministic turing machine

  - Decision problem : Yes / No Question
  - Examples:
    - Given a, b, and c the integers, is a + b = c?
    - Given p an integer, is p prime?

- NP : Set of decision problems, solvable in polytime
  with a nondeterministic turing machine
  - Equivalent to the “polytime – checkable” decision problems

TMI : P vs NP

LOOK AT ME I'M A GRAD STUDENT, I'M 30 YEARS OLD AND I MADE $600 LAST YEAR.
BART! DON'T MAKE FUN OF GRAD STUDENTS, THEY JUST MADE A TERRIBLE LIFE CHOICE.

- NP : Set of decision problems, solvable in polytime with a nondeterministic turing machine
  - Equivalent to the “polytime - verifiable” decision problems (Professor - Solvable problems)
- Examples:
  - Is there a Hamiltonian cycle in a given graph, whose length is smaller than X? *TSP

Other interesting Complexity Classes

- BPP (Bounded-error, Probabilistic, Polynomial)

Set of decision problems, can be guessed in guaranteed accuracy greater than ½.
The probability of “failure” is in both decision problems about **Yes** and **No**.

Ex : Primality testing (Miller - Rabin)
- In fact, Miller - Rabin is an RP algorithm.
- RP is a set of probs. **exact** in “No”; MR never mistakes prime for composite.

cf) Primality testing is P! (Agrawal, 2002)

Other interesting Complexity Classes

- co-NP

Set of decision problems which is easily verifiable for “answer no”

Unsolved : NP = co-NP ?

Invitation to CNT

Solving a simple problem.

Wait, is it really “simple”?

Task

Given a $n \times n$ integer matrix A. Evaluate $\det A$.

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

$$\det A = \sum_{\sigma} \operatorname{sgn}(\sigma) \cdot a_{1\sigma_1} a_{2\sigma_2} \cdots a_{n\sigma_n}$$

Adding $n!$ terms is too expensive.

Simplifying the task

- Determinant is invariant to the row-blending. (equiareal transform)

$$\det\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix} = \det\begin{pmatrix}3 & 5\\1 & 2\end{pmatrix}$$

- Determinant of an upper-diagonal matrix

$$\det\begin{pmatrix}u_{11} & \cdots & u_{1n}\\ \vdots & \ddots & \vdots\\ 0 & \cdots & u_{nn}\end{pmatrix} = u_{11}u_{22}\cdots u_{nn}$$

- Removing the lower triangle part by row-blending (Gaussian elim.) : $O(n^3)$. poly!

Gaussian elimination

- $\begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix} \to \begin{pmatrix} 2 & 1 \\ 0 & \frac{7}{2} \end{pmatrix}.$

- Rational Numbers?????????????????
  - The determinant will eventually be an integer (Guaranteed by the expanded formula).
  - But the denominator can grow up too large to handle during the rational operations.

Gaussian elimination

- Rational Numbers????????????????
- Big Prime method
  - $\frac{1}{a} \rightarrow a^*(\mathrm{mod}\, P)$!
  - All the intermediate values are confined in $[0, P)$, and they are all integers.

  - **Then, how large the prime $\boldsymbol{P}$ should be?**

Gaussian elimination

- **Then, how large the prime P should be?**
- The method should give the 'exact' determinant.
- The limit for the magnitude of determinant is:

$$M = \sum_{\sigma} |X|^n = n!\, X^n.$$

- Considering the negative range, $P \geq 2M$.
  - $\log P = \Omega(n \log n + n \log X)$, which is way too big.
  - The modular computation is not that expensive, but it is hard to find that big prime.

Chinese Remainder Theorem

- For n pairwise-coprime integers $m_1, m_2, \cdots, m_n$, given n congruence equations

$$\begin{gathered} x \equiv a_1 (m_1) \\ x \equiv a_2 (m_2) \\ \vdots \\ x \equiv a_n (m_n) \end{gathered}$$

- There exists a unique integer A modulo m, satisfies:

$$x \equiv A\ (m_1 m_2 \cdots m_n)$$

Chinese Remainder Theorem

- So it is enough to choose K primes, to make the product of them exceed $2M$.
- Since $p_1 p_2 \cdots p_K > 2^K$, no more than $\log 2M = O(n \log nX)$ primes are needed.
- Knowing $p_K \sim K \log K$ from $\pi(x) \sim \frac{x}{\log x}$, we can find K primes in near $O(K^2 \log^2 K)$ time, even with our worst method.
- Case closed! CRT made it.

Conclusion

1. Precompute K primes naively.

2. For each primes, obtain the modular-determinant by applying Gaussian Elimination.

3. Merge the mods by CRT.

4. Let D be the total modular (product of the primes).
    1. If $Ans > \frac{D}{2}$, return $Ans - D$.
    2. Else, return Ans.

Reviewing CRT

Is CRT just a “local trick” for integers?

Isomorphic structures

- Two structures S_1, S_2 are 'isomorphic' if there is a bijection $\hat{\phi} : S_1 \to S_2$, if all algebraic laws in S_1 is conserved in the language of S_2, even after being carried by $\hat{\phi}$.

- So, isomorphic structures are exactly "indistinguishable", which implies they are truly "identical".

- The same things are **really** the same.

CRT as an isomorphism

- For n pairwise-coprime integers $m_1, m_2, \cdots, m_n$, with $M \coloneqq m_1 m_2 \cdots m_n$, the following isomorphicity holds:

$$\mathbb{Z}/M\mathbb{Z} \approx (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})$$

$$\hat{\phi} : A \longmapsto (a_1, a_2, \cdots a_n)$$

Investigating ‘Coprimity’

- Let us consider the two coprime number a, b. The CRT – relation becomes

$$\mathbb{Z}/ab\mathbb{Z} \approx \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}.$$

- Clearly, $ab\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z},$ and $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.
  - Each of them is equivalent to $\gcd(a, b) = 1$.

- Two ‘substructure’s are coprime if and only if their ‘sum’ is the whole!
  - What is the ‘substructure’?
  - At first, what is the ‘whole structure’??

The ‘whole structure’ : Ring

- The structure $(R, +, \times)$ is a **ring** when the following are satisfied:
  - $(R, +)$ is an abelian. (associative, identity, inverse, commutativity)
  - $(R, \times)$ is a monoid. (associative, identity)

- $\mathbb{Z}, 8\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}$ are all rings.

The ‘substructure’ : Ideal

- For a ring R, $\boldsymbol{I \subset R}$ is called an ideal of R, when all the algebraic law of R works in I as well (in restricted version) and I ‘absorbs’ R by (left) multiplication.

  - $(I, +_R)$ is an abelian. (associative, identity, inverse, commutativity)
  - $(I, \times_R)$ is a monoid. (associative, identity)
  - For all $r \in R$ and $x \in I$, $rx \in I$.
  - Note that I can’t be empty, since I should include the identity.

- $8\mathbb{Z}$ is an ideal of $2\mathbb{Z}$, $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

- Is $\mathbb{Z}[i]$ an ideal of $\mathbb{C}$?

CRT as an isomorphism

- Let $\mathbb{a}, \mathbb{b}$ be ideals of R. $\mathbb{a}, \mathbb{b}$ are **coprime** if $\mathbb{a} + \mathbb{b} = R$.

- For coprime ideal $\mathbb{a}, \mathbb{b} \subset R$, the following CRT – law holds:

$$R/\mathbb{a} \cap \mathbb{b} \approx R/\mathbb{a} \times R/\mathbb{b}\,.$$

- The detailed proof will be written on the board.

Adding ‘factorization’ to the Ring

From Rings to Fields

Not gentle anymore

Polynomial factorization

- For a ring R, the **polynomial ring** $R[x]$ is a ring as well.

- For $\mathbb{Z}[x]$, the polynomial $x^2 - 1 = (x - 1)(x + 1)$ is uniquely factorized.

- But for $\mathbb{Z}_8[x]$, $x^2 - 1 = (x - 1)(x + 1) = (x - 3)(x + 3)$. 😠
  The factorization is not uniquely determined.

- So we add some 'RESTRICTION' to the rings to make them well – behaved.
  - We should define the 'prime' first – the fundamental elements of factorization.

Integral Domain

- A ring R is an *integral domain* if $ab = 0 \Rightarrow a = 0 \vee b = 0$ is guaranteed for all a, b.

- $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}/8\mathbb{Z}$ is not - since $2 \times 4 = 0$.

‘Prime’ Ideal?

- An integer p is prime if $x \mid p \Rightarrow x = 1 \vee x = p$.

- *An ideal* $I \subset R$ *is a prime ideal if* $I \subset J \Rightarrow J = I \vee J = R$ *..?*

‘Prime’ Ideal and ‘Maximal’ Ideal

- An integer $\boldsymbol{p}$ is prime if $\boldsymbol{p} \mid \boldsymbol{ab} \Rightarrow \boldsymbol{p} \mid \boldsymbol{a} \vee \boldsymbol{p} \mid \boldsymbol{b}$.

- An ideal $I \subset R$ is a **prime ideal** if $ab \in I \Rightarrow a \in I \vee b \in I$.
  - I is a prime ideal if R/I is an integral domain.
  - If pR is a prime ideal, p is called prime element of R.

- An ideal $\mathrm{I} \subset \mathrm{R}$ is called **maximal ideal** if $\mathrm{I} \subset \mathrm{J} \Rightarrow \mathrm{J} = \mathrm{I} \vee \mathrm{J} = \mathrm{R}$.

Necessity of the rigid definition of prime: a counterexample

- Let $R = \mathbb{Z}[x]$, and a prime ideal $I = (x)$.

- $I \subset J = (\{x, 2\})$, but J is neither I nor R. So I is not a maximal ideal.

cf) In $\mathbb{Z}[\sqrt{-5}]$, 3 is an irreducible number, but not a prime:

$$9 = 3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

- If we have both ‘primality’ and ‘maximality’,
  the unique factorization will be achieved!

PID：An overkill

- A ring R is a **principle ideal domain** if every ideal of R is *principle*;

  For all ideal $I \subset R$, there exists $a \in R$ such that $I = aR$.

- In PID, every prime ideal is maximal.

- All PID elements accept unique factorization into prime elements.

UFD：The desired

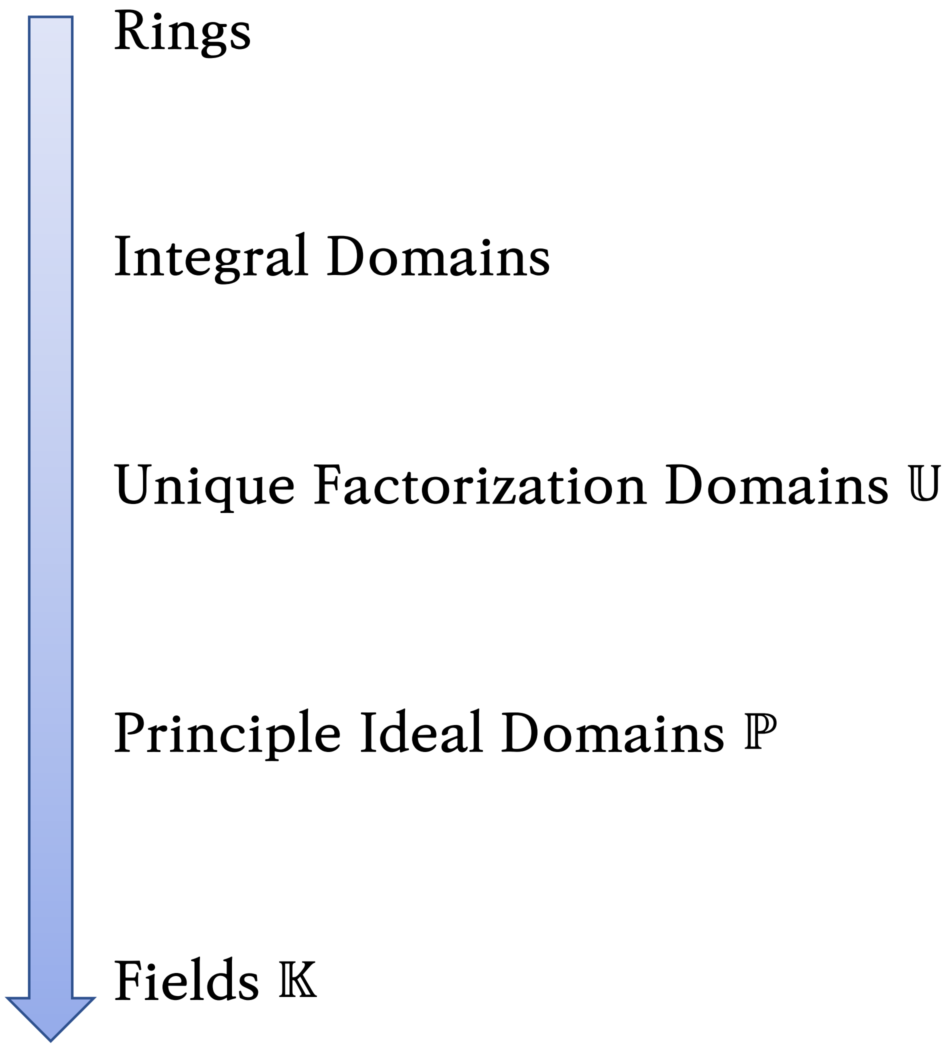
- A ring R is a **unique factorization domain** if every element has a unique factorization into its prime element.

- Every PID is UFD.
- Every UFD is not PID:
  - $\mathbb{Z}[x]$ and an ideal (p, x).
  - $\mathbb{K}[x, y]$ and an ideal (x, y).

FIELDS!

- A ring R is a **field** if $(R - \{0\}, \times)$ is an abelian.
- $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_p$ are fields.
- $\mathbb{Z}$ is not a field; 2 doesn't have multiplicative inverse.
- Fields are **simple**: there is no proper nontrivial ideal of a field.

Domains sorted with the order of restrictions



Rings

Integral Domains

Unique Factorization Domains $\mathbb{U}$

Principle Ideal Domains $\mathbb{P}$

Fields $\mathbb{K}$

〈Algebraic facts〉

- $\mathbb{U}[x]$ is also UFD.
- $\mathbb{P}$ is a UFD.
- $\mathbb{K}[x]$ is a PID.

Krull dimension: Classifying the factorization

- Krull dimension of a commutative ring is defined as **the maximal length** of its prime ideal tower.

- $0 \subset (p) \subset (p, x) \subset \mathbb{Z}[x]$, so Krull dimension of $\mathbb{Z}[x]$ is 2.
- Fields have Krull dimension 0.

- Rings with the same Krull dimension has similar factorization scheme, which will be discussed later.
  - $\mathbb{K}[x, y]$ is similar to $\mathbb{Z}[x]$?

Field Extension

Blackboard discussion..