Mid-Semester Wrap Up

Lecture 12
Topics to be covered

Basic tools for expressing ideas
- Logic, Proofs,
  Sets, Relations, Functions

- Basic tools for expressing ideas
  Recursion
  Induction
  Numbers and patterns therein

Bounding
big-O

- Counting

Trees

Graphs
Topics Covered

Basic tools for expressing ideas
Logic, Proofs,
Sets, Relations, Functions

Recursion
Induction
Numbers and patterns therein

Bounding big-O
Counting

Trees
Graphs
n people went to a Chinese restaurant, and sat on a large circular table, with a rotating disk in the centre.

Each one ordered a different dish. The servers brought all the dishes out at the same time and placed them on the disk, one in front of each person.

It turned out that no person had their dish in front of them.

Prove that they can rotate the disk in such a way that at least two diners will have their dishes in front of them.

For each person i, calculate $d_i$ the number of positions that the disk needs to be rotated clockwise to get to their dish.

$d_i \in \{1, \ldots, n-1\}$. $d_1, \ldots, d_n$. So at least two values $d_i, d_j$ which are equal. Rotate the disk by that much.
Given an arbitrary sequence of \( n \) integers \( a_1, \ldots, a_n \), there is some sequence of consecutive elements \( a_i, a_{i+1}, \ldots, a_{i+d} \) which sums up to a multiple of \( n \).

[e.g., \( a_1=4, a_2=2, a_3=7, a_4=4, a_5=2 \)]

First consider all \( n \) sequences starting with \( a_1 \), and let their sums be \( s_1, \ldots, s_n \).

[e.g., \( s_1=4, s_2=6, s_3=13, s_4=17, s_5=19 \)]

If any one of them is a multiple of \( n \), we are done.

Otherwise, \( r_i = \text{rem}(s_i, n) \) is in the range \([1,n-1]\) for each \( i \), and so by PHP, there are \( i, j \) s.t. \( i<j \) (w.l.o.g.) and \( r_i = r_j \pmod{n} \)

[e.g., \( s_1=4, s_5=19 \)]

Then, \( a_i + \ldots + a_j = s_j - s_i \) is a multiple of \( n \)

[2+7+4+2 = 15]
A generalisation of PHP: If \( n \) numbers \( x_1, \ldots, x_n \) add up to \( y \), then there is an \( i \) s.t. \( x_i \geq \frac{y}{n} \)

Because if all \( x_i < \frac{y}{n} \), then \( x_1 + \ldots + x_n < n \left( \frac{y}{n} \right) = y \)

“Everyone cannot be below average.”

Also true that \( \exists i \ x_i \leq \frac{y}{n} \)

For \( x_i \) being integers, can state as \( \exists i \ x_i \geq \left\lceil \frac{y}{n} \right\rceil \)

E.g., if \( y = n(r-1) + 1 \), \( \exists i \ x_i \geq r \)

Further generalisation: If \( x_1 + \ldots + x_n \geq r_1 + \ldots + r_n \), \( \exists i \) s.t. \( x_i \geq r_i \)
Euclidean algorithm to find gcd(a,b)

$(a_0,b_0) \leftarrow (a,b)$ where $a \geq b$

for $(i=0; b_i > 0; i++)$

$a_{i+1} \leftarrow b_i$ ; $b_{i+1} \leftarrow \text{rem}(a_i, b_i)$ ;

return $a_i$

Extended Euclidean algorithm to find $u,v$ s.t. $au+bv=\gcd(a,b)$

Idea: keep track of $u_i,v_i$ s.t. $b_i = u_i a + v_i b$.

Let $q_i = \lfloor a_i/b_i \rfloor$ so that $b_{i+1} = a_i - q_i b_i$

$u_0=0, v_0=1$. $u_1=1, v_1=-q_0$ (because $b_1 = a - q_0 b$)

For $i \geq 1$, recall $a_i = b_{i-1} = u_{i-1} a + v_{i-1} b$.

So, $b_{i+1} = a_i - q_i b_i = (u_{i-1} a + v_{i-1} b) - q_i (u_i a + v_i b)$

$u_{i+1} = u_{i-1} - q_i u_i$. $v_{i+1} = v_{i-1} - q_i v_i$. 

<table>
<thead>
<tr>
<th></th>
<th>$a_i$</th>
<th>$b_i$</th>
<th>$q_i$</th>
<th>$u_i$</th>
<th>$v_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20</td>
<td>9</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>9</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>-2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>-4</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Numbers**

**Totient Function**

\[ \varphi(m) = |\mathbb{Z}_m^*|, \text{ where } \mathbb{Z}_m^* = \{ a \mid \gcd(a, m) = 1 \} \]

- e.g., for \( p \) prime, \( \varphi(p) = p-1 \)

\[ \forall a \in \mathbb{Z}_m^*, \; a^{\varphi(m)} \equiv 1 \pmod{m} \]

\[ 2^{2019} \pmod{100} = ? \]

\[ 2 \not\in \mathbb{Z}_{100}^*, \text{ so can't use Euler's theorem directly} \]

\[ 2^{2019} \equiv 2^{\text{rem}(2019, \varphi(25))} \pmod{25} \]

\[ \varphi(25) = 5(5-1) = 20. \; \text{And, } 2019 \equiv -1 \pmod{20}. \]

\[ 2^{2019} \equiv 2^{-1} \equiv 13 \pmod{25}. \]

\[ 2^{-1} \pmod{m} \text{ for odd } m \text{ is } (m+1)/2 \]

Solve for \( x \) s.t. \( x \equiv 13 \pmod{25}; \; x \equiv 0 \pmod{4} \).

Multiple of 4 in \( 13, 38, 63, 88 = 88 \)
Important Fact (won’t prove): If \( p \) is a prime, then
\[ \exists g \in \mathbb{Z}_p^* \ \forall x \in \mathbb{Z}_p^* \ \exists k, \ 0 \leq k < p-1, \ x = g^k \]

Such a \( g \) is called a “generator of \( \mathbb{Z}_p^* \)”

Consequence: Can analyse \( \mathbb{Z}_p^* \) by considering it as \( \{1, g, g^2, \ldots, g^{p-2}\} \), with exponents from \( \mathbb{Z}_{p-1} \) (because \( g^{p-1} = 1 \))

e.g., How many generators?

Fix one generator \( g \). Elements of \( \mathbb{Z}_p^* \) are \( 1, g, g^2, \ldots, g^{p-2} \)

\( g^t \) is a generator iff \( \{1, g, g^2, \ldots, g^{p-2}\} = \{1, g^t, g^{2t}, \ldots, g^{(p-2)t}\} \) (mod \( p \))

i.e., \( \{0, 1, \ldots, p-2\} = \{0, t, \ldots, (p-2)t\} \) (mod \( p-1 \))

i.e., \( \gcd(t, p-1) = 1 \)

\( \varphi(p-1) \) such \( t \)

Number of generators of \( \mathbb{Z}_p^* = \varphi(p-1) \)
Poset

- Partial order: Reflexive, Anti-Symmetric, Transitive
- e.g., Divisibility poset \((\mathbb{Z}^+,\leq): a \leq b \text{ iff } a|b\)

- a covered by b (a \lessdot b)
  - iff a \leq b, a \neq b, and there is no x s.t. a \leq x \leq b
- \lessdot is the reflexive and transitive closure of \leq

- Hasse diagram: the graph for \leq (with edges pointing upwards, so that the arrow is implicit)
A lattice is a poset in which every pair of elements \( \{a,b\} \) has a greatest lower bound and a least upper bound.

Implies the same for every finite set of elements

\[
g.l.b.(\{a,b,c\}) = g.l.b.( \{g.l.b.(\{a,b\}), c\} )
\]

Let \( z = g.l.b.( \{a,b\} ) \) (which exists).
\[
x \in \text{LowerBd}(\{a,b,c\}) \implies x \in \text{LowerBd}(\{a,b\}) \implies x \preceq z;
\]
so \( x \in \text{LowerBd}(\{z,c\}) \).

Conversely, if \( x \in \text{LowerBd}(\{z,c\}) \), \( x \preceq z \preceq a, x \preceq z \preceq b, x \preceq c \).

i.e., \( \text{LowerBd}(\{a,b,c\}) = \text{LowerBd}(\{z,c\}) \).

But RHS has a greatest element. So LHS does too: \( g.l.b.(\{a,b,c\}) \)

e.g., Divisibility poset (g.l.b. is g.c.d., l.u.b. is l.c.m.), subsets poset (g.l.b. is intersection, l.u.b. is union)
Chains

Consider poset \((S, \preceq)\)

- \(C \subseteq S\) is called a chain if \(\forall a, b \in C\), either \(a \preceq b\) or \(b \preceq a\)

- \(\text{height}(a) = \max C\) chain with \(a\) as maximum \(|C|\)

- Height of a poset = \(\max C\) chain \(|C|\)

- Height of poset = \(\max_{a \in S} \text{height}(a)\)

- A maximal chain is a chain which is not contained in a longer chain

- Suppose \(C\) is a finite maximal chain. The greatest element of \(C\) exists and is a maximal element of the poset. The least element of \(C\) exists and is a minimal element of the poset
Mirsky's Theorem

- $A \subseteq S$ is called an anti-chain if $\forall a,b \in A$, $a \preceq b \rightarrow a = b$

- Given a poset of height $H$, the least number of anti-chains needed to partition $S$ is $H$

- Need at least $H$ anti-chains to partition $S$

- Consider a chain of length $H$ (exists). No two elements in that chain can be in one anti-chain

- And need no more: use $\{ A_h \mid h=1,\ldots,H \}$, where $A_h \triangleq \{ a \mid \text{height}(a)=h \}$

- $A_h$ is an anti-chain $\leftarrow$ Why?

- $\{ A_h \mid h=1,\ldots,H \}$ is a partition $\leftarrow$ Why?
Mirsky's Theorem: Example

Given a poset of height $H$, the least number of anti-chains needed to partition $S$ is $H$

Claim: Any poset with $n$ elements must have either (i) a chain and an anti-chain both of size equal to $\sqrt{n}$ or (ii) a chain or an anti-chain of size greater than $\sqrt{n}$

Suppose (ii) doesn't hold. All chains, anti-chains of size $\leq \sqrt{n}$. So, height of poset, $H \leq \sqrt{n}$.
By Mirsky, can partition the poset into $H$ anti-chains, say of sizes $n_1,...,n_H$. So, $n = n_1 + ... + n_H$.
But $n_i \leq \sqrt{n}$. So $n \leq H \sqrt{n}$. Thus $H = \sqrt{n}$. Then, each $n_i = \sqrt{n}$. So (i) holds.
Mirsky’s Theorem: Example

Consider the numbers from 1 to n arranged in an arbitrary order on a line. There must exist a \( \sqrt{n} \)-long subsequence of that is completely increasing or completely decreasing as you move from right to left.

Consider poset \([n], \preceq\) defined as: \( a \preceq b \) if \( a \leq b \) and \( a \) appears not “later than” (left of) \( b \) in the line

Verify poset!

Chain: An increasing subsequence (right to left)

Anti-chain: If \( a \) appears before \( b \), but not \( a \preceq b \), then \( a > b \). So a decreasing sequence (right to left)

Previous claim: Chain or anti-chain of length at least \( \sqrt{n} \)
Bijections: Infinite sets

e.g., \( f: \mathbb{Z} \rightarrow \mathbb{Z} \) defined as \( f(x) = -x \)

\( f \) is a bijection

A set \( S \) is countably infinite if there is a bijection from \( S \) to \( \mathbb{Z} \)

e.g., set of even integers \( E \). \( f: E \rightarrow \mathbb{Z} \) where \( f(x) = x/2 \), is a bijection

“Two countably infinite sets are only as numerous as one”

e.g., there is a bijection \( f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \)

“How?“

“How?“

“How?“

“Countably infinitely many countably infinite sets are only as numerous as one”

(We will return to this later)