## MATH 113: DISCRETE STRUCTURES
## FINAL EXAM REVIEW

- Trees
  - Definition: connected acyclic graph.
  - Trees have leaves.
  - Trees can be grown.
  - Trees with $n$ vertices have $n-1$ edges.
  - Cayley's theorem: The number of labeled trees with $n$ vertices is $n^{n-2}$.
  - Prüfer codes.
- Catalan numbers
  - Catalan number $C_n$ counts unlabelled full binary trees with $n+1$ leaves.
  - Catalan recurrence: $C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}$.
  - Closed formula: $C_n = \frac{1}{n+1}\binom{2n}{n}$.
  - Other structures counted by Catalan numbers:
    - Dyck paths.
    - Parenthesizations.
    - Temperley–Lieb diagrams.
- Probability theory
  - Basic objects: sample space, events, probability distribution.
  - Uniform distribution on a finite sample space.
  - Independent events.
  - Conditional probability $P(A|B)$.
  - Bayes' Law: $P(B|A) = P(A|B)P(B)/P(A)$.
  - Law of Total Probability: $P(A) = \sum_i P(A|B_i)P(B_i)$ for $\{B_i\}$ a partition.
  - Random variables.
  - Expected value $E(X)$.
  - Linearity of expected value: $E(cX+Y) = cE(X) + E(Y)$.
  - Special types of random variables:
    - Bernoulli.
    - Binomial.
    - Indicator.
- Number theory
  - Divisibility.
  - Prime numbers.
  - Fundamental theorem of arithmetic (unique prime factorization).
  - Infinitude of primes.
  - Prime number theorem: $\pi(n) \sim n/\log n$.
  - Fermat's little theorem: $p | a^p - a$.
  - Greatest common divisors and Euclidean algorithm.
  - Congruences.
  - Multiplicative inverses modulo $n$.
  - Euler $\phi$ function: $\phi(n) = |\{r \in \mathbb{N} \mid r < n \text{ and } \gcd(r,n) = 1\}|$.
  - Euler's formula: $\phi(n) = n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_k)$ for $n$ with prime factors $p_1, \ldots, p_k$.

*Problem* 1. Suppose that the vertices of a graph have degrees $4, 1, 1, 1, 1$. Decide whether this graph is a tree, is not a tree, or could be a tree or non-tree and prove your assertion. What if the vertex degrees are $3, 3, 2, 1, 1$?

*Solution.* First consider the case with degrees $4, 1, 1, 1, 1$. There are $5$ vertices, one of which has degree $4$; this vertex must be adjacent to the other four vertices. This already gives the remaining vertices degree $1$, so we have determined the graph: it's a star, which is a special kind of tree.

If the vertex degrees are $3, 3, 2, 1, 1$, then

$$2|E| = \sum_{v \in V} \deg v = 3 + 3 + 2 + 1 + 1 = 10,$$

so there are $5$ edges. A tree on $5$ vertices as $4$ edges, so this graph cannot be a tree. □

*Problem* 2. Suppose that $2n$ people are seated around a circular table. In how many ways can they simultaneously shake hands with another person at the table so that none of their arms cross each other? Draw pictures of the $n = 1, 2, 3$ cases, come up with a conjecture, and prove it.

*Solution.* By deforming the table into a square with $1, 2, \ldots, n$ on the top edge and $2n, 2n-1, \ldots, n+1$ on the bottom, we see that non-crossing handshakes correspond to a Temperley–Lieb diagram on $2n$ nodes. Thus there are $C_n$ ways for the group to shake hands without crossing. □

*Problem* 3. For a permutation $\sigma$ of $\underline{2n}$, let $X(\sigma)$ be the number of $i \in \underline{2n}$ such that $\sigma(i) > 2i$. Determine the expected value of $X$.

*Solution.* For $i \in \underline{n}$ let $\chi_i$ be the indicator variable such that

$$\chi_i(\sigma) = \begin{cases} 1 & \text{if } \sigma(i) > 2i, \\ 0 & \text{if } \sigma(i) \leq 2i. \end{cases}$$

Then $X = \sum_{i=1}^{2n} \chi_i$ and we may compute its expected value as

$$E(X) = \sum_{i=1}^{2n} E(\chi_i) = \sum_{i=1}^{2n} P(\sigma(i) > 2i).$$

Note that it is impossible for $\sigma(i) > 2i$ for $i \geq n$, so we can rewrite this sum as $\sum_{i=1}^{n-1} P(\sigma(i) > 2i)$. For a fixed $i \in \underline{n-1}$, $P(\sigma(i) > 2i) = \frac{2n-2i}{2n} = \frac{n-i}{n}$ [justify this!], so

$$E(X) = \sum_{i=1}^{n-1} \frac{n-i}{n} = \frac{1}{n} \sum_{j=1}^{n-1} j = \frac{1}{n} \cdot \frac{(n-1)n}{2} = \frac{n-1}{2}.$$

□

*Problem* 4. For $a, b, c, n \in \mathbb{Z}$ suppose that $ac \equiv bc \pmod{n}$. Let $d = \gcd(c, n)$ and prove that

$$a \equiv b \pmod{n/d}.$$

*Solution.* Suppose that $ac \equiv bc \pmod{n}$. Then there exists $k \in \mathbb{Z}$ such that $ac - bc = kn$. Dividing by $d = \gcd(c, n)$, we get

$$a(c/d) - b(c/d) = k(n/d)$$

where $c/d, n/d \in \mathbb{Z}$. It follows that

$$a(c/d) \equiv b(c/d) \pmod{n/d}.$$

Observe that $\gcd(c/d, n/d) = 1$, so $c/d$ has a multiplicative inverse in $\mathbb{Z}/(n/d)\mathbb{Z}$. Multiplying by this number produces the congruence $a \equiv b \pmod{n/d}$. □