MATH6222 Week 8 Lecture Notes

Rui Qiu

2017-04-24

1 Monday

Viewing times

Apr. 26 10:30-11:30, 3:00-4:00
Apr. 27 1-2
Apr. 28 10:30-11:30, 3:00-4:00

Midterm questions

Hand-deck probability $(5,4,3,1,) \to \frac{4\binom{13}{5}3\binom{13}{4}2\binom{13}{3}13}{\binom{52}{13}}$

But for $(5,4,4,0) \to \frac{4\binom{13}{5}\binom{3}{2}\binom{13}{4}^2}{\binom{52}{13}}$

Bug-path problem

Suppose that $|a|+|b| \leq k, a, b$ have the same parity as k.

Then the bug can reach (a,b) on day k.

Clearly, the bug can walk to (a,b) in $|a|+|b|$ days. (By walking a steps up/down if $a+/-$, and b steps right/left if $b+/-$).

Note if k has same parity as $a+b$, then it also has same parity as $|a|+|b|$.

Thus, $k-(|a|+|b|)$ is divisible by 2.

If the bug walked up and down $\frac{k-(|a|+|b|)}{2}$?... then it lands on (a,b) on day k.

...

If (a,b) denotes the current position of the bug, then $|a|+|b|$ changes by at most 1 each day. Thus on day k, $|a|+|b| \leq k$.

For parity, note that, the parity of $a+b$ changes every day, either from odd to even or from even to odd.

Thus the parity of $a+b$ is always the same as the parity of the day k.

Problem: Determine all integers satisfying $x^2 \equiv 1 \mod 5$.

$1,4,6,9,11,14,16,19,21,24,26,29\ldots$

- any integer where last digit is $1,4,6,9$
- all integers in congruence classes $1,4,6,9 \mod 10$

- all integers in congruence classes $\overline{1}, \overline{4} \mod 5$

Note: If x, y are in same congruence class $\mod 5$, then $x^2 \equiv y^2 \mod 5$.

Just need to figure out which congruence classes $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} \to \{\overline{0}, \overline{1}, \overline{4}, \overline{4}, \overline{1}\}$

$$\mathbb{Z}_5$$

So solution is just all integers in these 2 congruence classes $\overline{1}, \overline{4} \mod 5$

$2x = 5 \mod 5$ has no solutions in $\mathbb{Z}_6$.

Key Question: Given working $\mod n$, given congruence class $\overline{a}$. When can we find a $\overline{c}$ such that $\overline{c} \cdot \overline{a} = 1$?

2 Thursday

Proposition: Fix $n \in \mathbb{N}$. Suppose $a \in \mathbb{Z}$ satisfies $(a, n) = 1$. Then $\exists\, b \in \mathbb{Z}$ such that $ab = 1 \mod n$.

Furthermore, b is unique up to congruence $\mod n$. Equivalently, if $(a, n) = 1$, then $\overline{a} \in \mathbb{Z}_n$ has a unique multiplicative inverse: $\exists\, !\overline{b} \in \mathbb{Z}_n$ such that $\overline{a}\overline{b} = 1$.

Notation: $(a, b) = \gcd(a, b)$.

Lemma: Given $a, b, n \in \mathbb{Z}$, and suppose $(a, n) = 1$. If $n | ab$, then $n | b$.

Proof: $(a, n) = 1$ means a and n have no prime factors in common. Therefore, the set of all prime factors of n is contained in the set of all $1, \ldots, ab$.

...

Proof of Proposition: Consider multiples of $a \mod n$:

$$\{0 \cdot a, 1 \cdot a, 2 \cdot a, \ldots, (n-2) \cdot a\} = \{i \cdot a : 0 \leq i \leq n-1\}$$

Claim: These n integers are all distinct $\mod n$.

$ia \equiv ja \mod n \iff n | (ia - ja) \iff n | a(i - j) \iff n | (i - j)$

(Use lemma in the last step)

This is impossible, because i, j are distinct integers between 0 and $n-1$. Therefore $i - j \neq 0$ and $|i - j| \leq n - 1$, so $i - j$ cannot be divisible by n.

This says we have a bijection from $\mathbb{Z}_n \to \mathbb{Z}_n$ by $\overline{x} \to \overline{ax}$.

Since there are only n congruence classes $\mod n$, every congruence class appears in this set

$$\{ia : 0 \leq i \leq n-1\}$$

Therefore $\overline{1}$ is represented by some integers in this set:
We have $i \cdot a \equiv 1 \mod n$ for some $0 \leq i \leq n-1$.

Second Proof: By Euclidean algorithm,
$\exists\ k, l \in \mathbb{Z}$ such that $ka + ln = 1 \iff ka \equiv 1 \mod n$
Suppose we are working with $\mod 17$, find $\overline{5}^{-1}$.
$17 = 3 \times 5 + 2, 5 = 2 \times 2 + 1, 2 = 17 - 3 \times 5$.
$1 = 7 \times 5 - 2 \times 17$.
$7 \cdot 5 \equiv 1 \mod 17$
$5x \equiv 3 \mod 17$
$x \equiv 7 \cdot 5x \equiv 7 \cdot 3 \mod 17 \equiv 4 \mod 17$.

Observation: If p is prime, then $1, \ldots, p-1$ are all relatively prime to p.

- This implies that **every** non-zero congruence class in $\mathbb{Z}_p$ has a multiplication inverse.
- $ax \equiv b \mod p$ ($a \not\equiv 0 \mod p$) has a unique solution $\mod p$.

Fermat's Little Theorem: Let p be a prime. If $a \in \mathbb{Z}$ and $a \not\equiv 0 \mod p$, then $a^{p-1} \equiv 1 \mod p$.

Proof: Consider non-zero multiples of a: $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$. These are distinct and non-zero $\mod p$.
Multiply: $(1 \cdot a) \cdot (2 \cdot a) \cdots (p-1) \cdot a \equiv (p-1)! \mod p$
$\implies a^{p-1} \equiv 1 \mod p$.
Example (modulo 7): $5 \cdot 10 \cdot 15 \cdot \cdots \cdot 30 \equiv 6! \mod 7$

Wilson's Theorem: Let p be a prime. Then $p|[(p-1)! + 1]$.
Example: $p = 5, [(p-1)! + 1] = 25, 5|25$.

Proof: In fact, $(p-1)! \equiv -1 \mod p$. (Try to prove this as a key step.)
$\overline{a} = 1, 2, 3, 4, 5, 6$
$\overline{a}^{-1} = 1, 4, 5, 2, 3, 6$
$6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \equiv 6 \cdot 1 \cdot 1 \cdot 1 \equiv -1 \mod 7$

Lemma: Fix p prime, let $a \in \mathbb{Z}$ ($a \not\equiv 0 \mod p$). Then $a^2 \equiv 1 \mod p \iff a \equiv 1 \mod p$ or $a \equiv -1 \mod p$.

Proof: $a^2 \equiv 1 \mod p \iff p|(a^2-1) \iff p|(a-1)(a+1) \iff p|(a-1)$ or $p|(a+1) \iff a \equiv 1 \mod p$ or $a \equiv -1 \mod p$.

Proof of Wilson's Theorem: Each of the integers $2, \ldots, p-2$ pairs off with a unique inverse. Thus $2 \cdot 3 \cdots \cdot (p-2) \equiv 1 \mod p$. Then $(p-1)! \equiv (p-1) \equiv -1 \mod p$. We are done.

3 Friday: Some miscellaneous

3.1 Permutations

How many swaps do we need from 6-5-4-3-2-1 to 1-2-3-4-5-6?

3 swaps. 6 to 1, 5 to 2, then 4 to 3. How would you prove that you cannot do this in 2 swaps. If you have $2n$ numbers out of position, you at least need n number of swaps to make then right. (Each swap changes at most 2 positions.)

How many swaps do we need from 2-3-4-5-6-1 to 1-2-3-4-5-6?
5 swaps.
2-3-4-5-1-6
2-3-4-1-5-6
2-3-1-4-5-6
2-1-3-4-5-6
1-2-3-4-5-6
But how to prove that 4 or 3 swaps cannot make this?

Definition: A **permutation** of $[n] : \{1, 2, \ldots, n\}$ is a bijection $f : [n] : [n]$.

The *word form* of a permutation is the list $f(1), f(2), \ldots, f(n)$.

A *transposition* is just a permutation which swaps i and j (some $i, j \in [n]$) but leaves all other entries the same. Let σ_{ij} := transposition swapping integers i, j.

Let f be the permutation associated to some out of order list. We seek a sequence of transpositions $\sigma_{i_1,j_1}, \sigma_{i_2,j_2}, \sigma_{i_3,j_3}, \ldots$ such that

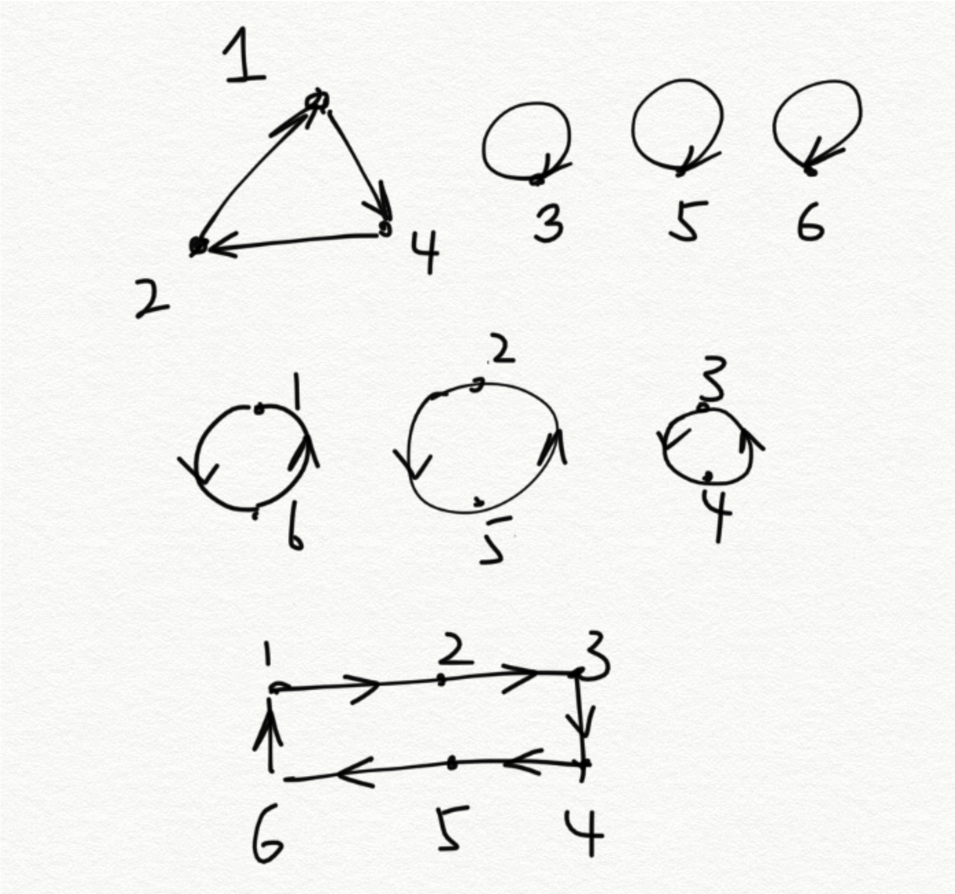
$$\sigma_{i_k,j_k} \circ \sigma_{i_2,j_2} \circ \cdots \circ \sigma_{i_1,j_1} \circ f = \text{identity function}$$

$f(i) = j, f(j) = i, f(k)$, for all $k \neq i, j$.

Remark: Every transposition is its own inverse.

Therefore, $\iff f = \sigma_{i_1,j_1} \circ \sigma_{i_2,j_2} \circ \cdots \circ \sigma_{i_k,j_k}$.

Permutation is a map $f : [n] \to [n]$. So generally, given a function $f : A \to A$, we define the functional digraph of f to be a graph with a vertex for every $a \in A$ and arrow from $f(a) \to f(a), \forall a \in A$.



Given a permutation f whose digraph has k cycles, the minimal number of swaps to sort it is $n - k$.

Proposition: composing a permutation f with a transposition $\sigma_{i,j}$, changes the digraph by adding 1 cycle if i, j are on the same cycle, deleting 1 cycle if i, j are on different cycles.

3.2 Relation

Let S be a set. An **relation** on S is a subset $R \subseteq S \times S$.

Example:

$\{(x, y) : x \leq y\} \subseteq R \times R$ "$\leq$" relation on R.

$\{(a, b) : a|b\} \subseteq \mathbb{N} \times \mathbb{N}$ "divisibility relation".

Let S be the set of all sets.

$\{(A, B) : A \subseteq B\} \subseteq S \times S$

$\{(A, B) : \exists \text{ bijection } A \to B\} \subseteq S \times S$

Fix $n \in \mathbb{N} : \{(a, b) : a \equiv b \mod n\} \subseteq \mathbb{Z} \times \mathbb{Z}$

Fix a permutation $f : \{(a, b) : f^k(a) = b \text{ some } k \in \mathbb{N}\} \subseteq [n] \times [n]$

An **equivalence relation** is a relation which satisfies:

1. $\forall x \in S, (x, x) \in R$. (reflexive)
2. $\forall x, y \in S, (x, y) \in R \implies (y, x) \in R$. (symmetric)
3. $\forall x, y, z \in S, (x, y) \in R$ and $(y, z) \in R \implies (x, z) \in R$. (transitivity)

If R is an equivalence relation, then for any $x \in S$, we can consider the "equivalence class" of x. Notation:

$$\overline{X} = [x] = \{y \in S : y \sim x\}$$

Think about "congruence class" in modulo arithmetic.