COMS BC3262: Introduction to Cryptography

Lecture 14: Midterm Recap and Cyclic Groups

March 23, 2026

Office Hours

Office hours:

- **Eysa**: Mondays 3-5, Milstein 512
- **Mark**: Tuesdays 6:30-8:30, Milstein 503

This week there may be an extra review session on Friday to review topics from the first half of the course (tentatively 2pm, location TBD)

- Completely optional but highly recommended for anyone who feels iffy on anything we covered before spring break
- Hosted by one of last semester's intro crypto TAs

Midterm Stats

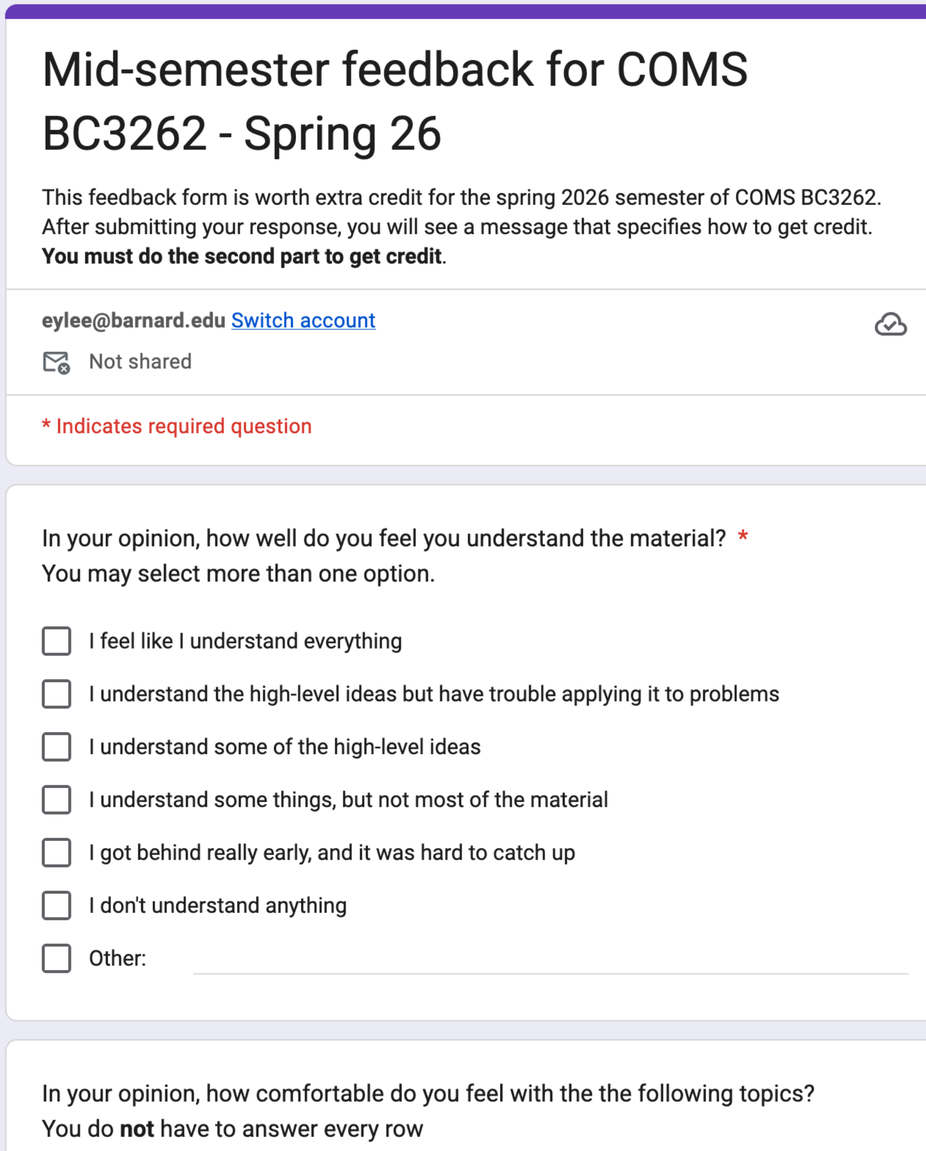
- 100 points possible (90 points + 10 extra credit)
  - 3 people scored [90,100] (1 of which was a perfect score)
  - 5 people scored in [70, 90)
  - 8 people scored [40, 70)
  - 5 people scored below 40
- Mean and median were both about 60
- (This is not including people who did not take the exam)

Alternate Oral Exam

- There is an optional oral exam from March 24 - April 3
  - For each question that you earned less than 50% of the possible points (not including extra credit), the oral exam is an opportunity to earn *up to* 50% credit on that question
  - Questions will be formatted to test conceptual understanding of the topics from the first half of the course
    - For example, “explain what ___ means”
- Please see EdStem post for the link to schedule

Mid-Semester Feedback

- There is an optional extra credit mid-semester feedback survey worth 1 point on the midterm
  - There is only 1 required question and a few other optional questions
  - I've already gotten valuable feedback (thank you!) that I hope to incorporate
  - I'm waiting until the poll closes to go over the results
- The feedback form closes on Thursday
  - You *must* send the follow-up email specified on the Google form confirmation page in order to get extra credit



Mid-semester feedback for COMS BC3262 - Spring 26

This feedback form is worth extra credit for the spring 2026 semester of COMS BC3262. After submitting your response, you will see a message that specifies how to get credit. **You must do the second part to get credit**.

eylee@barnard.edu Switch account

Not shared

* Indicates required question

In your opinion, how well do you feel you understand the material? *
You may select more than one option.

- [ ] I feel like I understand everything
- [ ] I understand the high-level ideas but have trouble applying it to problems
- [ ] I understand some of the high-level ideas
- [ ] I understand some things, but not most of the material
- [ ] I got behind really early, and it was hard to catch up
- [ ] I don't understand anything
- [ ] Other:

In your opinion, how comfortable do you feel with the the following topics?
You do **not** have to answer every row

Problem Sets

- PS 4 won’t be released until April 1 (next week Wednesday)
- Unfortunately I have a small grading backlog…
  - PS 3 won’t be graded for a bit longer

Here’s my cat being cute as an apology

Today’s Lecture

- Recap of some basic number theory

- Discrete Log

Recall: Groups

Groups

Definition: A group is a set $\mathbb{G}$ along with a binary operation $\circ$ satisfying

- **Closure**: $\forall g, h \in \mathbb{G}$, it holds that $g \circ h \in \mathbb{G}$
- **Identity element**: $\exists 1_{\mathbb{G}} \in \mathbb{G}$ such that $\forall g$ it holds that $g \circ 1_{\mathbb{G}} = 1_{\mathbb{G}} \circ g = g$
- **Inverse element**: $\forall g \, \exists g^{-1}$ such that $g \circ g^{-1} = g^{-1} \circ g = 1_{\mathbb{G}}$
- **Associativity**: $\forall g_1, g_2, g_3 \in \mathbb{G}$ it holds that $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$

Groups

Definition: A group is a set $\mathbb{G}$ along with a binary operation $\circ$ satisfying

- **Closure**: $\forall g, h \in \mathbb{G}$, it holds that $g \circ h \in \mathbb{G}$
- **Identity element**: $\exists 1_{\mathbb{G}} \in \mathbb{G}$ such that $\forall g$ it holds that $g \circ 1_{\mathbb{G}} = 1_{\mathbb{G}} \circ g = g$
- **Inverse element**: $\forall g \, \exists g^{-1}$ such that $g \circ g^{-1} = g^{-1} \circ g = 1_{\mathbb{G}}$
- **Associativity**: $\forall g_1, g_2, g_3 \in \mathbb{G}$ it holds that $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$

- Denote by $|\mathbb{G}|$ the cardinality of $\mathbb{G}$. If $\mathbb{G}$ is finite, this is the number of elements.
- $|\mathbb{G}|$ is the order of $(\mathbb{G}, \circ)$
- $(\mathbb{G}, \circ)$ is commutative (Abelian) if $\forall g, h \in \mathbb{G}$ it holds that $g \circ h = h \circ g$
- $(\mathbb{H}, \circ)$ is a sub-group of $(\mathbb{G}, \circ)$ if $(\mathbb{H}, \circ)$ is a group and $\mathbb{H} \subseteq \mathbb{G}$

Groups

Definition: A group is a set $\mathbb{G}$ along with a binary operation $\circ$ satisfying

- **Closure**: $\forall g, h \in \mathbb{G}$, it holds that $g \circ h \in \mathbb{G}$
- **Identity element**: $\exists 1_{\mathbb{G}} \in \mathbb{G}$ such that $\forall g$ it holds that $g \circ 1_{\mathbb{G}} = 1_{\mathbb{G}} \circ g = g$
- **Inverse element**: $\forall g \, \exists g^{-1}$ such that $g \circ g^{-1} = g^{-1} \circ g = 1_{\mathbb{G}}$
- **Associativity**: $\forall g_1, g_2, g_3 \in \mathbb{G}$ it holds that $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$

- Is $(\mathbb{Z}, +)$ a group?
- Is $(\mathbb{Z}, \cdot)$ a group?
- Is $(\mathbb{R}, +)$ a group?
- Is $(\mathbb{R}, \cdot)$ a group?
- Is $(\mathbb{R}^*, \cdot)$ a group, where $\mathbb{R}^* = \mathbb{R} \backslash \{0\}$?

Group Exponentiation

Given $g \in \mathbb{G}$, we can consider applying the group operation on g multiple times: $((g \circ g) \circ g \ldots) \circ g$

- This is called group exponentiation
- In multiplicative notation we write $g^m = g \cdot \ldots \cdot g$
  - Not to be confused with integer multiplication/exponentiation
- We define $g^0 = 1$ and $g^{-m} = (g^{-1})^m$
- $g^{m_1} \cdot g^{m_2} = g^{m_1+m_2}$
- If $\mathbb{G}$ is commutative, then $(gh)^m = g^m \cdot h^m$

Groups

Theorem: Let $\mathbb{G}$ be a finite group of order $m = |\mathbb{G}|$. Then, for every $a \in \mathbb{G}$, it holds that $a^m = 1$

Corollary: Let $\mathbb{G}$ be a finite group of order $m = |\mathbb{G}| > 1$. Then, for every $g \in \mathbb{G}$ and every integer x it holds that $g^x = g^{[x \bmod m]}$

In general, if you want to exponentiate, it helps to figure out the order of the group first and then perform modular reduction

The Group $(\mathbb{Z}_N, +)$

The group $(\mathbb{Z}_N, +)$ for $N > 1$

- Consider the set $\mathbb{Z}_N = \{0, \ldots, N-1\}$ with the operation addition $\bmod N$
- **Closure**: By definition, for $a, b \in \mathbb{Z}_N$, it holds that $[a + b \bmod N] \in \mathbb{Z}_N$
- The **identity** element is $[0 \bmod N]$
- The (additive) **inverse** of $a \in \mathbb{Z}_N$ is $[N - a \bmod N]$
- Associativity and commutativity follow from these properties in the integers

The Group $\mathbb{Z}_N^*$

- Is $(\mathbb{Z}_N, \cdot\ )$ a group?
  - No! Not every element has an inverse
  - For example, 2 is not invertible in $\mathbb{Z}_4$
- What are the invertible elements in $\mathbb{Z}_{10}$?

$$\mathbb{Z}_{10} = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}$$

The Group $\mathbb{Z}_N^*$

- Is $(\mathbb{Z}_N, \cdot)$ a group?
  - No! Not every element has an inverse
  - For example, 2 is not invertible in $\mathbb{Z}_4$
- What are the invertible elements in $\mathbb{Z}_{10}$?

$$\mathbb{Z}_{10} = \{1, 3, 7, 9\}$$

The Group $\mathbb{Z}_N^*$

- For $N > 1$, define $\mathbb{Z}_N^* = \{a \in \{1,\ldots,N-1\} \mid \gcd(a,N) = 1\}$ with the group operation $ab = [ab \bmod N]$
- $\mathbb{Z}_N^*$ is a commutative group
  - **Closure**: If $a, b \in \mathbb{Z}_N^*$, then $[ab \bmod N]$ has inverse $[b^{-1}a^{-1} \bmod N]$
  - **Identity**: 1 is the identity element
  - **Inverse**: If $a \in \mathbb{Z}_N^*$, i.e., $\gcd(a,N) = 1$, then $Xa + YN = 1$ and $a^{-1} = [X \bmod N]$
  - **Associativity** and **commutativity** follow from these properties in the integers

The Group $\mathbb{Z}_N^*$

Euler's phi function / Euler's totient function: $\phi(N)$ is the order of $\mathbb{Z}_N^*$

e.g., $\phi(N) = |\mathbb{Z}_N^*|$

Cyclic Groups

Cyclic Groups

Definition: Let $\mathbb{G}$ be a finite group of order m and let $g \in \mathbb{G}$. Then

- $\langle g \rangle = \{g^0, g^1, g^2, \ldots\}$
- The order of g (denoted $\mathrm{ord}(g)$) is the smallest $0 < i \leq m$ such that $g^i = 1$

Facts:

- $\langle g \rangle$ is a subgroup of $\mathbb{G}$ (called “the subgroup generated by g”)
- $\langle g \rangle = \{g^0, g^1, g^2, \ldots, g^{\mathrm{ord}(g)-1}\}$
- $g^x = g^y$ if and only if $x = y \bmod m$
- The order of g divides the order of $\mathbb{G}$, i.e., $\mathrm{ord}(g) \mid m$

Cyclic Groups

Example: $\mathbb{Z}_{15}^{*} = \{1,2,4,7,8,11,13,14\}, \ |\mathbb{Z}_{15}^{*}| = 8$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle =$

Cyclic Groups

Example: $\mathbb{Z}_{15}^{*} = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^{*}| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle =$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle = \{1,7,4,13\}$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle = \{1,7,4,13\}$
- $\langle 4 \rangle =$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle = \{1,7,4,13\}$
- $\langle 4 \rangle = \{1,4\}$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle = \{1,7,4,13\}$
- $\langle 4 \rangle = \{1,4\}$
- $\langle 11 \rangle =$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle = \{1,7,4,13\}$
- $\langle 4 \rangle = \{1,4\}$
- $\langle 11 \rangle = \{1,11\}$

Cyclic Groups

Definition: A group $\mathbb{G}$ is cyclic if there exists $g \in \mathbb{G}$ such that $\mathbb{G} = \langle g \rangle$. In this case, g is called a generator of the group

- $(\mathbb{Z}_N, +)$ is cyclic with generator 1

Theorem: A group $\mathbb{G}$ with prime order is cyclic and every $g \in \mathbb{G} \backslash \{1\}$ is a generator

Theorem: If p is prime then $(\mathbb{Z}_p^*, \cdot)$ is cyclic

Note: $\mathbb{Z}_p^*$ is *not* a prime order group (unless $p = 3$) since it is order $p - 1$

Cyclic Groups

Consider $(\mathbb{Z}_p^*, \cdot)$ for a prime p. This is a cyclic group for some g:

$$\mathbb{Z}_q^* = \{1,\ldots,p-1\}$$

Cyclic Groups

Consider $(\mathbb{Z}_p^*, \cdot)$ for a prime p. This is a cyclic group for some g:

$$\mathbb{Z}_q^* = \{1,\ldots,p-1\} = \{g^1, g^2, \ldots, g^{p-1}\}$$

Cyclic Groups

Consider $(\mathbb{Z}_p^*, \cdot)$ for a prime p. This is a cyclic group for some g:

$$\mathbb{Z}_q^* = \{1,\ldots,p-1\} = \{g^1, g^2, \ldots, g^{p-1}\} = \{g^0, g^1, \ldots, g^{p-2}\}$$

Cyclic Groups

Consider $(\mathbb{Z}_p^*, \cdot)$ for a prime p. This is a cyclic group for some g:

$$\mathbb{Z}_q^* = \{1,\ldots,p-1\} = \{g^1, g^2, \ldots, g^{p-1}\} = \{g^0, g^1, \ldots, g^{p-2}\} = \langle g \rangle$$

Cyclic Groups

Consider $(\mathbb{Z}_p^*, \cdot)$ for a prime p. This is a cyclic group for some g:

$$\mathbb{Z}_q^* = \{1, \ldots, p-1\} = \{g^1, g^2, \ldots, g^{p-1}\} = \{g^0, g^1, \ldots, g^{p-2}\} = \langle g \rangle$$

Note that this group is isomorphic to $(\mathbb{Z}_{p-1}, +)$

- Can define bijection $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ as $f(x) = g^x \mod p$ (for a generator g)
  - $f(0) = g^0 = g^{p-1} = 1 \mod p$
  - $f(1) = g^1, \ldots$

Cyclic Groups

Claim: Let $\mathbb{G}$ be a cyclic group of order m, and let g be a generator. Then the mapping $f : \mathbb{Z}_m \to \mathbb{G}$ defined by $f(x) = g^x$ is an isomorphism

Cyclic Groups

Mathematically $(\mathbb{Z}_p^*, \cdot)$ and $(\mathbb{Z}_{p-1}, +)$ are the same. But computationally they're not necessarily!

- While $f(x) = g^x \bmod p$ is efficiently computable, the inverse f^{-1} is believed not to be!

- This is known as the "Discrete log assumption" (DLA) for $\mathbb{Z}_p^*$

Next Time

- Discrete Log, CDH, DDH