Course Digest

MATH 558, Fall 2020

Introductory Modern Algebra

Date. Tuesday, November 24

Notices. Welcome to our last day of class, and thanks for making this a successful semester together! We will hold **one lecture**, from **1 – 2:15 pm**, and all are welcome to attend! We will have enough space to social distance.

Tasks.

Videos ⟶ Find the link below to today's lecture, and to the solutions for our final two quizzes.

- The Fundamental Theorem of Algebra
- Quiz 9 solutions
- Quiz 10 solutions

Course survey ⟶ Please fill out our KU Course Survey for MATH 558 when you get a chance. Course surveys are open until December 6.

Teammate evaluation ⟶ Please submit an evaluation for your teammates, like last time, today on Blackboard.

Investigation modules ⟶ If you aren't already finished, you'll be done with your last module tonight. Congrats! You can find your graded and annotated CRT module on Blackboard. If you forgot to submit the name of your team, email me and I can send you your graded module. Corrections (which as you know, are optional) for the CRT module are due on Tuesday of Study Week, and corrections for the final module are due on Thursday of Study Week.

Office hours ⟶ Office hours this week were yesterday and today from 4–5 pm. Please email me by Saturday with any requests for Office Hours during Study Week. They will be posted on the course website.

Final Exam ⟶ Our Final Exam times are as follows:

- 11 am section: Wednesday, December 9, 10:30 am – 1 pm
- 1 pm section: Tuesday, December 8, 1:30 – 4 pm

Some useful notes:

(1) Our exam is **cumulative**, but is focused more on the material that has yet to be tested on.

(2) The best way to study for the exam is to practice, practice, practice problems! You can use those from investigation modules, from homework, and from quizzes.

(3) A review sheet with material covered after Midterm 2 will be posted on the course website at the beginning of Study Week.

(4) The format of the Final Exam is the same as for the midterms.

(5) Though it is longer than the midterms, you will have more time per problem on the Final than on the midterms!

Problems ⟶ Chapter 14, #15, 16, 24, 27. Moreover, please factor the following polynomials as a product irreducible polynomials in $\mathbb{R}[x]$, and then in $\mathbb{C}[x]$:

(1) $f(x) = x^3 - 1$.
(2) $g(x) = x^4 + 5x^2 + 4$.
(3) $h(x) = x^4 + 1$. (Hint: Find $\sqrt{i}$ in $\mathbb{C}$.)

Reading ⟶ None!

Synopsis. We covered our final topic today, the Fundamental Theorem of Algebra. It says that every polynomial over the real numbers can be factored "all the way down" to the product of linear polynomials over the complex numbers. In other words, the irreducible polynomials over the complex numbers are exactly the degree 1 polynomials. We illustrated this idea by factoring polynomials in $\mathbb{R}[x]$ into irreducible ones in $\mathbb{C}[x]$.

Date. Thursday, November 19

Notices.

- We will offer **one** in-person lecture next Tuesday, since some of us who regularly come in person will be out of town. **Class will run from 1:00–2:15 pm** in our classroom (Mallot, 6th floor of the Kansas Union), and both the 11 am and 1 pm classes are welcome to join!
- I am so impressed with you guys during this challenging semester! You have worked hard and mastered important algebraic concepts. Keep it up!

Tasks.

Videos ⟶ Check out the following videos covering today's material. Note that the second and third are good supplemental resources in working through our last Investigation Module:

- Roots of polynomials
- Unique factorization of polynomials
- The field of complex numbers

Course survey ⟶ Please fill out our KU Course Survey for MATH 558 when you get a chance. Course surveys are open until December 6.

Office hours ⟶ Please email me with any requests if you have preferred times for Office Hours for next week (Monday or Tuesday) by Saturday, and for Office Hours during study week before the following Saturday.

Problems ⟶ Chapter 14, #10(i), 34, 37, 41, 42, 45, 46; Chapter 15, #8, 9

Reading ⟶ Please read 15D, 15F before our last class period on Tuesday!

Synopsis. Today we started by pushing the Division Algorithm for polynomials over a field further, to study roots of polynomials. This was then useful in studying factorization of polynomials into reducible ones; like for integers, we have a Unique Factorization statement for polynomials over a field! Finally, we gave a short introduction to the complex numbers $\mathbb{C}$, which form a field.

Date. Tuesday, November 17

Notices.

- Our class will be online on Thursday.
- We won't have a quiz on Thursday, in fact, you have completed all quizzes for the semester! Remember that your two lowest quiz scores will be dropped.
- It is highly encouraged that your investigation module group meets during our Thursday class period to start our last module. The module will really help solidify your knowledge of our last class topic–polynomials rings!

Tasks.

Investigation module ⟶ Our final module, Divisibility in Polynomial Rings, is due next Tuesday. This semester, many students have found the modules to strengthen their understanding of class topics, and often in MATH 558 students wish they had gotten more practice on our final topic, polynomial rings, before the final exam. We will have no more quizzes this semester so that you have more time for the module.

Videos ⟶ A video of today's lecture is available on Mediahub:

Division algorithm for polynomials

Course survey ⟶ I (and I'm sure, your other professors) would really appreciate it if you make sure to fill out our course survey for MATH 558 when you get a chance. These surveys are open until December 6.

Office hours ⟶

- Office hours this week are today and tomorrow (Tuesday and Wednesday) from 9–10 am.
- We *will* offer office hours next week (before Thanksgiving) and the week after that. Please email me with any requests on times by the Saturday before the respective week.

Problems ⟶ Chapter 13, #4, 5; Chapter 14, #1, 2, 4, 5, 7, 8

Reading ⟶ Please read sections 14B–14C for next time.

Synopsis. Today we delved deeper into the study of polynomial rings, studying the degree of a product of polynomials, the Division Algorithm for polynomials, and the notion of divisibility for polynomials. We noticed that the properties in polynomials over fields because more nicely in some ways than in polynomial rings over arbitrary fields (e.g., those that have zero divisors!).

Date. Thursday, November 10

Notices.

- We will hold an in-person class next Tuesday.
- Office hours next week will be from 9–10 am on both Tuesday and Wednesday.
- To get a rough estimate of your current course grade, average your two Midterm letter grades. Of course, the Investigation Modules and Final Exam can also pull up your score! If you have any concerns about your status in the class, please let me know; the final drop deadline is next week Wednesday, November 18.

Tasks.

Quiz ⟶ Please find, complete, and submit Quiz 10, accessible on Blackboard.

Videos ⟶ Please watch the following video, which introduces the topic we will build upon for the remainder of the semester: Introduction to polynomial rings

Office hours ⟶ Let me know by tomorrow if you have requests for Office Hours times next week, and I will do my best to incorporate them!

Problems ⟶ Chapter 12, #3, 10, 11, 12 and Chapter 13, #1, 2

Reading ⟶ Please re-read 13B, and read 14A.

Synopsis. Today, we introduced the notion of polynomials over a commutative ring, i.e., polynomials with coefficients coming from a fixed ring. We investigated the fact that the set of all these polynomials, using the familiar methods for addition and multiplication of polynomials, form a commutative ring themselves!

Date. Tuesday, November 10

Notices. Our class on Thursday will be hosted online. There will be a quiz on the RSA Cryptosystem. Stay careful out there!

Tasks.

Midterm 2 ⟶ Please make sure to look over the comments on your graded midterm, available on Blackboard. The scale and solutions are also available via our Course Digest entry from last time. Feel free to stop by Office Hours with questions.

Investigation module ⟶ We've extended your Chinese Remainder Theorem module to be due (any time) on Friday. Like last time, every team member should input a "submission" to Blackboard. Note that a typo in part 3(d) has been corrected–the modulus there should be mn instead of m.

Office hours ⟶ Office hours this week are from 3:30–4:30 pm today, and 10:30–11:30 am tomorrow. Look forward to chatting with some of you soon!

Videos ⟶ See the video of the lecture on today's topic: RSA Cryptosystem

Problems ⟶ Problems 1–3 in Section 10.2 the Savin text

Reading ⟶ Please read Section 10.2 in the Savin text, and 13A–13B in Childs, by Thursday.

Synopsis. Today we further study the Euler phi function, and then used it to describe and investigate the RSA Cryptosystem, a modern method of encrypting data that is extremely important to our day-to-day lives!

Date. Thursday, November 5

Notices. We will hold an in-person session on Tuesday, November 10. Hope to see some of you there!

Tasks.

Quiz ⟶ Please find, complete, and submit Quiz 9 on Blackboard during your class period today. The quiz should take about 10 minutes to complete.

Investigation module ⟶ Your next Investigation Module is now available; it is on the Chinese Remainder Theorem, and is due next Thursday. (I think you'll enjoy it!) Please email each other today to set up your first meeting.

Videos ⟶ Check out the video on today's topic: Euler's Theorem

Midterm 2 ⟶

- The class, overall, did quite well on our second midterm! I'm impressed with your dedication to the course, especially with the extra challenge of a hybrid course.
- Watch the Midterm 2 solutions video to brush up on anything you missed, and feel free to come to office hours with questions.
- If you'd like to boost your final grade, remember that the Investigation modules constitute 20%, and the Final Exam 25%, so there is still room to improve!
- The median score on Midterm 2 is 39.5/55 (72%), and here is its letter-grade scale (again, the fact that the percentages don't add to 100 is due to rounding):

Grade	Range	% students
A	40–55	50%
B	34–39	24%
C	27–33	24%
D	0–26	3%

Office hours ⟶ Office hours this week will be by appointment; feel free to email me if you'd like to meet!

Problems ⟶ Chapter 9, #42–44, 46, 49, 52

Reading ⟶ Please read 12A and 12C before next time.

Synopsis. Last time, we noticed that Fermat's little theorem can fail if we replace the prime p with a composite integer. In today's session, we introduce another theorem that addresses the case of composite moduli! In fact, this theorem, called Euler's theorem, encompasses Fermat's little theorem as a special case. This theorem allows for much simpler modular arithmetic computations (modulo any integer, not just primes), and as we will see next time, has important applications in cryptography!

Date. Tuesday, November 3

Notices.

- It is election day, so (carefully!) go out and exercise your right to vote if you are eligible!
- Our Midterms should be graded soon, so look out for an email when the scale is ready. The scale, and solutions, will be posted in the Course Digest.
- Class on Thursday will be online, and we will likely hold a quiz during the class period, so check back then!

Tasks.

Videos ⟶ See the video from today's lecture here: Fermat's Little Theorem

Investigation modules ⟶ A new Investigation Module will be assigned soon. There will be a couple changes in groups, mostly due to at least one group losing a member. If you have any concerns about your team, please let me know by tomorrow at noon.

Office hours ⟶ Office hours this week will be by appointment. Send me a quick email with some times when you are available if you'd like to meet.

Problems ⟶ Chapter 9, #18–22, 27–29

Reading ⟶ Please read 9C by Thursday.

Synopsis. Today, we studied Fermat's little theorem. We did some examples to explore what it says, and investigated its consequences on the orders of integers modulo primes p. We also proved the theorem using facts we know about the ring $\mathbb{Z}/p\mathbb{Z}$!

Date. Thursday, October 27

Notices. We will likely offer an in-person lecture again next time; check back on Monday for confirmation.

Tasks.

Investigation module corrections ⟶ Corrections for our most recent module are due Monday.

Office hours ⟶ Let me know if there are times next week that are best for you for Office Hours.

Videos ⟶ A video of today's lecture is available on Mediahub:

Zero divisors, units, and orders of units

Problems ⟶ Chapter 7, #27–34

Reading ⟶ Please read 9A–9B before next time.

Synopsis. Today we investigated the zero divisors and units of $\mathbb{Z}/m\mathbb{Z}$. We proved the cancellation law by nonzerodivisors, and showed that no unit of a commutative ring is both a unit and a zero divisor. We formally classified the units and zero divisors of $\mathbb{Z}/m\mathbb{Z}$. We also defined a field as a commutative ring in which all nonzero elements are units; we proved that $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime. Finally, we defined the order of a unit in a finite commutative ring. Throughout, we illustrated the definitions and properties through examples.

Date. Tuesday, October 27

Notices. We will have an in-person lecture offered on Thursday, October 29.

Tasks.

Midterm 2 ⟶ Access our first exam on Blackboard, and submit it before the end of your regularly-scheduled class period. Remember that late exams will not earn credit. Good luck!! You can do it!

Investigation module corrections ⟶ Remember that your third module's corrections are due next Monday.

Date. Thursday, October 22

Notices. Remember that Midterm 2 will be held online, during class, this upcoming Tuesday. Make sure you are comfortable using your scanning app, since late exams cannot be accepted!

Tasks.

Quiz ⟶ You will earn full credit on the quiz today as long as you follow the steps outlined below. The quiz is meant to prepare you for the upcoming midterm, so you will get the most out of it if you take the quiz without looking at any resources!

(1) Access Quiz 8 on Blackboard and complete it as usual.
(2) Watch the Quiz 8 solutions video. Then use a different color (if possible, or use a pen instead of a pencil), mark all incorrect steps on your completed quiz, and explain the correct ones, as if you are grading someone else's quiz. We expect that most of you will miss some steps, which is part of the learning process! You will still receive full credit for the quiz.
(3) Turn in your corrected quiz, with markings, to Blackboard.

Midterm 2 ⟶ As you know, our second midterm is on Tuesday (October 27); see our Midterm 2 Conceptual Review.

Office hours ⟶ Today we have Office Hours from 4–5 pm, and on Monday from 9:30–11 am. See the course website for the Zoom links.

Videos ⟶ Please watch the following videos, which cover today's material.

(1) More on rings
(2) Midterm 2 review problems

Reading ⟶ Please re-read 7C before class next Thursday.

Synopsis. Today we get practice proving statements about rings, and introduce the notion of a zero divisor of an arbitrary ring. We also go through some problems related to the material on our upcoming midterm.

Date. Tuesday, October 20

Notices.

- Heads up: Midterm 2 is a week from today, with the same format as last time. Remember that late exams will not earn credit. The final topic covered on the exam is the notion of rings.
- Please check back to see if an in-person session will be offered on Thursday. Whether in class or online, we will go over some review problems for the midterm, and discuss rings in more depth.

Tasks.

Investigation modules ⟶

- If you were not the scribe on the most recent Investigation Module, and you did not make a "dummy" submission including only your team name, please do so now! This is how the grader will recognize the score that should be entered.
- Please let me know by email ASAP if you have any major concerns about the participation of your Investigation Module teammates. In MATH 558, our main goal is for all to learn!

Midterm 2 ⟶

- Start catching up with any homework problems you haven't completed, since Midterm 2 is a week from today!
- Please refer to the Midterm 2 Conceptual Review to help with your studying.
- You can also study quiz problems you missed using the videos below.

Quiz solutions ⟶ Solutions to the quizzes you've taken since Midterm 1 are available:

- Quiz 7 solutions
- Quiz 6 solutions
- Quiz 5 solutions (Note that this quiz is mislabeled as Quiz 4.)

Office hours ⟶ This week, Office Hours will be from 10–11 am on Wednesday and 4–5 pm on Thursday.

Videos ⟶ Videos from today's lecture are available here:

(1) More on groups
(2) Intro to rings

Problems ⟶ Chapter 7, #1, 3, 5–7, 12

Reading ⟶ Please read 7C by Thursday.

Synopsis. We first reviewed the notion of a group, and some of their features, which we proved last time. After this, we defined a ring, which builds on the idea of a group, but provides a broader framework in which to solve more complicated equations (those analogous to the algebra problems we've all solved earlier in life). We gave several examples of rings (and some non-examples), and then started practicing proving properties of rings.

Date. Thursday, October 15

Notices.

- We will hold an in-person class on Tuesday. Looking forward to it! The videos from class will be posted later that afternoon.
- It's been a great semester so far with you all! Keep in mind that our second midterm is a week from Tuesday. Keep up the hard work!

Tasks.

Quiz ⟶ Please find Quiz 7 on Blackboard; as usual, it is due at the end of your class period. Good luck!

Investigation module ⟶ Remember that our third Investigation Module is due this evening (any time before midnight). Please remember that everyone must make a submission (with your team name), but only the scribe should submit your report and solutions.

Office hours ⟶ Please let me know if you have requests for Office Hours times next week.

Videos ⟶ Please watch the following videos, covering our new (and abstract!) topic of groups. Next time we will move to the notion of rings, which are extensions of groups, so getting the idea here is important!

(1) Intro to groups
(2) Examples of groups
(3) Proofs of properties of groups

Problems ⟶ Chapter 7, #8, 9, 15

Reading ⟶ Please read 7A by next time.

Synopsis. Today we introduced the notion of a group, which is a number system where we can solve certain equations. We gave examples of groups, many of which we are very familiar with. Then we proved some properties that groups have.

Date. Tuesday, October 13

Notices.

- Our class on Thursday will be online. We may have a quiz, so make sure to check in here during your class period!

- If you are in the 11 am lecture, please review the definition of the multiplicative identity from video (2) below. If you are in the 1 pm lecture, please see the final example in video (3), which we did not get to at the end of class!
- Note that a hint for one of our Investigation Module problems can be found below!

Tasks.

Investigation module ⟶ Our investigation module on Arithmetic in $\mathbb{Z}/m\mathbb{Z}$ is due on Thursday.

- Please remember that everyone needs to make a Blackboard assignment submission, but only the scribe should submit your team's solutions!
- Hint for 1(c): To avoid induction, first come up with a conjecture for the least nonnegative residues for $1^k, 2^k, \ldots, 5^k$ modulo 5, depending on the remainder when k is divided by 4. Prove it, and then apply your result to conclude for which k these form a CSR!

Office hours ⟶ Office hours this week are from 11 am–12 pm on Monday, and today from 4–5 pm.

Videos ⟶ Please refer to the following videos covering today's lecture:

(1) Review of $\mathbb{Z}/m\mathbb{Z}$
(2) Units in $\mathbb{Z}/m\mathbb{Z}$
(3) Solving equations in $\mathbb{Z}/m\mathbb{Z}$

Problems ⟶

Chapter 6, #42, 44, 47, 48, 61, 62

Reading ⟶ Please read 6C–6F by Thursday.

Synopsis. Today we confirm that congruence modulo m is an equivalence relation, and introduce $\mathbb{Z}/m\mathbb{Z}$, the set of all equivalence classes under this relation; we refer to these specific equivalence classes as congruence classes. Then we start investigating how to perform arithmetic on these congruence classes.

Date. Thursday, October 8

Notices. We will hold an in-person class on Tuesday. Have a nice weekend!

Tasks.

Quiz ⟶ Please complete Quiz 6, posted on Blackboard, during your regularly-scheduled class period.

Investigation module ⟶ Our third investigation module on Arithmetic in $\mathbb{Z}/m\mathbb{Z}$ is due next Thursday. Please meet your team today–the module covers most of today's material! If you have time, try to watch the short videos posted below before your meeting.

Investigation module corrections ⟶ Corrections on our Euclidean Algorithm module are due tonight. You can earn up to half the points you missed–it's a good way to pull up your course grade, little by little! Make sure to follow the guidelines, posted earlier in the Course Digest.

Office hours ⟶ Please email me by Sunday at 5 pm if you have a preference for Office Hours times next week.

Videos ⟶ Most of today's material is covered in your new investigation module. The following short videos introduce the initial topics:

(1) Congruence modulo m is an equivalence relation
(2) Intro to $\mathbb{Z}/m\mathbb{Z}$

Problems ⟶ Chapter 6, #5-8

Reading ⟶ Please read 6B–6C by next time.

Synopsis. Today we confirm that congruence modulo m is an equivalence relation, and introduce $\mathbb{Z}/m\mathbb{Z}$, the set of all equivalence classes under this relation; we refer to these specific equivalence classes as congruence classes. Then we start investigating how to perform arithmetic on these congruence classes.

Date. Tuesday, October 6

Notices. Thursday's class will be online, where we will have a quiz. There will be a few short videos, which we encourage you to watch before meeting your Investigation Module team, if possible.

Tasks.

Investigation modules ⟶

- The new Investigation Module is on the topic of Arithmetic in $\mathbb{Z}/m\mathbb{Z}$. If you have time, try to watch the short videos that will be posted on Thursday before you meet your team.
- You should have received an email with the contact info of your new team members. Plan your first meeting by Thursday–for instance, you could meet after completing the quiz. First order of business: come up with a new team name, which is related to math in some way!
- Updated submission instructions: Remember to put the team name on the top of both your report and your solutions, and list the full names of your teammates on the report. The scribe should still submit the final PDF including both of these. In addition, now each team member must also submit a "solution" that only consists of your team name.
- The module is due on Thursday, October 15 (at midnight).

Midterm 1 ⟶

- An overview on the outcome of the midterm with studying tips, can be found in the video Midterm 1 outcomes and tips. Solutions are detailed in Midterm 1 solutions.

- Comments on your own solutions are available on Blackboard.
- The average score on Midterm 1 is 42/60, a perfect 70%, which is remarkable on a challenging exam. The letter-grade scale for the midterm is as follows:

Grade	Range	% students
A	46–60	28%
B	40–45	33%
C	34–39	28%
D	30–33	10%

Office hours ⟶ Office hours this week are on Wednesday from 12:30–2 pm; the Zoom info is on the course website. Feel free to come to discuss midterm solutions, or any other course material.

Videos ⟶ Videos of today's lecture are available here:

(1) More practice on computations modulo m
(2) Equivalence relations

Problems ⟶

- Chapter 5, #7, 12, 22
- Chapter 1, #2, 3

Reading ⟶ Please read 6A by Thursday.

Synopsis. Today we practice doing computations modulo m, and then turned to the notion of equivalence relations. We detail their definition, and go through several examples and non-examples. We also introduced the concept of equivalence classes.

Date. Thursday, October 1

Notices.

- Notice that two tasks below are due by the end of our class period today!
- The first video from last time had some issues; please check out the new version posted.

Tasks.

Quiz ⟶ Please find Quiz 5 linked in Blackboard, and complete it before the end of our regularly-scheduled class period.

Investigation modules ⟶

- During this class period, please complete the Teammate Evaluation, which can be found on Blackboard.
- Your module on the Euclidean Algorithm will be graded later today, which means that corrections are due next Thursday.

Midterm 1 ⟶

- Your graded midterms are available on Blackboard.

- Please read the grading comments carefully; this will be useful for your future studying, and for getting solid up on Midterm 1 material, which will be used throughout the course.
- The average score on Midterm 1 is 42/60, a perfect 70%, which is remarkable on a challenging exam. The letter-grade scale for the midterm is as follows:

Grade	Range	Percentage of students
A	46–60	28%
B	40–45	33%
C	34–39	28%
D	30–33	10%

  (The percentages don't add to 100 due to rounding.) If you are close to a boundary between two letter grades, you can think of your grade as having a +/-, as appropriate. Your score, not your letter grade, will be used to calculate your final grade.
- Make sure to watch the video going over the Midterm 1 solutions if you have questions on any of the problems.
- Please let me know on Monday at noon if you have requests for Office Hours this week; I will do my best to accommodate the majority of students. You are welcome to ask questions about midterm problems, or new material.
- Remember that the best way to prepare for Midterm 2 is to keep up with assigned homework; as you can see from Midterm 1, exam problems cover the same material at a similar level. You can use Office Hours and Piazza as tools!

Office hours ⟶ If you have preferences for Office Hours times for next week (e.g., if you would like to come discuss midterm problems), please let me know by Monday at noon.

Videos ⟶ The following videos cover today's class material:

(1) Midterm 1 Solutions
(2) Least nonnegative residues modulo m
(3) Basic properties of congruence modulo m
(4) Calculations modulo m

Problems ⟶ Chapter 5, #9, 11, 15–17

Reading ⟶ Before next class period, please read Section 5B and Chapter 1.

Synopsis. Today, we established several useful properties of congruence modulo an integer $m > 1$, and got some practice doing calculations mod m.

Date. Tuesday, September 29

Notices.

- Our session will be online on Thursday, September 30. We will have two assignments (a quiz and a survey) that should be completed during your regular class period.

- Midterm 1 will be graded this week. Keep an eye on Blackboard for comments, and here for the letter-grade scale.

Tasks.

Videos ⟶ The following videos cover today's class material:

1. Divisibility in terms of prime factorizations
2. Existence of infinitely many primes
3. $\sqrt{2}$ is irrational
4. Introduction to congruence modulo m

Office hours ⟶ Our Office Hours this week are:

- 9–10 am on Wednesday
- 9–10 am on Thursday

As usual, Zoom info will be posted on the MATH 558 website.

Problems ⟶

- Chapter 4, #4, 10, 13, 43
- Chapter 5, #1, 3, 4, 6

Piazza ⟶ As Midterm illustrated, it is essential to keep up with homework problems as they are assigned. My advice is to have all problems completed one week after they are assigned. Since some are more difficult than others, and we are all different, this likely means that office hours and our Piazza discussion board will be useful!

Reading ⟶ Before Thursday's class period, please read Sections 4C and 5A.

Synopsis. Today, we get more practice using prime factorizations to investigate properties of integers. We also showed that there are infinitely many prime numbers! Finally, we introduced the notion of congruence modulo an integer $m > 1$.

Date. Thursday, September 24

Notices. We will have an in-person lecture on Tuesday, September 29.

Tasks.

Midterm 1 ⟶ Access our first exam on Blackboard, and submit it before the end of your regularly-scheduled class period. Good luck!

Investigation module corrections ⟶ Your corrections are due today. Remember to follow the guidelines to received up to half the points you missed!

Date. Tuesday, September 22

Notices.

- Midterm 1 is on Thursday during class, taken online.

- Be sure to complete the quiz sometime today (see below) to become oriented with the format and expectations for the exam! No exams submitted after the deadline can be accepted.

Tasks.

Quiz ⟶ Complete Quiz 4 sometime today, which can be accessed on Blackboard. The first part of the quiz will familiarize you with the exam guidelines and submission instructions, so pay careful attention, and let me know if you have any questions on them before Thursday.

Piazza ⟶ Remember that we are using Piazza as a collaborative tool to get answers on concepts quickly! Feel free to ask, or help answer a question. If you have trouble finding the link sent by email, follow this link. Please follow our Piazza guidelines.

Videos ⟶ See the video going over Quiz 3 below, and two additional videos covering today's topics, recorded in one of our in-person lectures today.

(1) Quiz 3 mistakes and solutions
(2) Midterm 1 review problems
(3) The utility of prime factorizations

Midterm Conceptual Review ⟶ Feel free to use the Conceptual Review as a study aid. It lists course topics, goals, and some extra practice problems.

Office hours ⟶ Our Office Hours this week are:

- 12–1 pm on Monday
- 3:30–4:30 pm on Tuesday
- 11 am–12 pm on Wednesday

As usual, Zoom info is posted on the MATH 558 website.

Investigation modules ⟶ Remember that your first Investigation Module corrections are due on Thursday. This is a good way to study for the exam! To receive credit, make sure to follow the guidelines linked in Thursday's digest entry.

Problems ⟶ Chapter 4, #14, 16, 17, 19–21, 30, 37

Reading ⟶ Before class next week on Tuesday, please read Sections 4A–4B.

Synopsis. Today we did some practice problems on topics that will be covered in Midterm 1. Then we discussed some useful ways to use prime factorizations in understanding divisibility properties, and proved that there are infinitely many primes.

Date. Thursday, September 17

Notices.

- Our Tuesday class will be hosted in person. We will do some review for the midterm, and then move on to a new topic.

- Make sure to complete the tasks in Tuesday's Course Digest entry that day; you will learn how Thursday's exam will run, and be submitted. Please remember that we cannot accept late exams!

Tasks.

Videos ⟶ Along with the reading, the following instructional videos constitute today's material. Note that the first two videos review Tuesday's, and the second investigation module's, material. For this reason, the videos will be posted after the quiz.

(1) Another example of the Euclidean and Extended Euclidean Algorithm
(2) Another example of solving a linear Diophantine equations
(3) The Property of Primes
(4) Unique factorization and the Fundamental Theorem of Arithmetic

Quiz ⟶ Please complete Quiz 3 during our regular class period.

Midterm ⟶ Our first midterm is in a week, on Thursday, September 24. The best way to study is to complete the homework assigned (as well as quiz and Investigation Module question), and quiz yourself on it. You might want to meet your Investigation Module team to study!

Midterm review ⟶ A conceptual review on the material covered on Midterm 1 is available; see Midterm 1 Conceptual Review.

Office hours ⟶ Please email me by Sunday at 5 pm if you have requests for Office Hours times next week, before our exam on Thursday. They will be posted on the course website.

Investigation modules ⟶

- Our next module will be assigned after the midterm. Note that some of our teams will change due to some students leaving our class. If you have requests on teammates (including current ones), please email me, and I will do my best to accommodate them.
- You should have received grades and feedback on the Induction module. Students are permitted to submit corrections to each module, following the guidelines here: Investigation module correction guidelines. Submissions should be written up individually, though you are highly encouraged to meet with your team to discuss them.

Problems ⟶

- Chapter 3, #35, 39 (use EEA, not EEA matrix), 57, 64
- Chapter 4, #1, 2, 5

Reading ⟶ Before next time, please read Section 4B in Childs.

Synopsis. We first did some review, practicing the Euclidean Algorithm, Extended Euclidean Algorithm, and solving linear Diophantine equations. Then we introduced the notion of prime factorizations, and proved their existence and uniqueness in the Fundamental Theorem of Arithmetic.

Date. Tuesday, September 15

Notices.

- Our first midterm will be next Thursday, September 24. The exam will be administered online; check the digest next Tuesday for information on the format of the exam. The best way to study is to complete all homework problems that have been assigned.
- Your first investigation modules should be graded soon. Watch for an email with details.
- Our Thursday class will be hosted online.

Tasks.

Videos ⟶ The following instructional videos cover the material from today:

(1) Quiz 2 mistakes and solutions
(2) Example of the Euclidean Algorithm and its Extended version
(3) Homogeneous linear Diophantine equations
(4) Solving linear Diophantine equations

Investigation module ⟶ Our second module is due tomorrow at 5 pm.

Quiz ⟶ We will have a quiz on Thursday. Make sure you know how to perform the Euclidean Algorithm, and the statement of Bézout's theorem!

Office hours ⟶ We will have office hours on Wednesday from 10–11 am. Please email me if you have requests for office hour times for next week (keeping in mind that our midterm is on Thursday).

Problems ⟶ Chapter 3, #58, 60–62, 65

Reading ⟶ Before next time, please read Section 4A in Childs.

Synopsis. Today, we defined linear Diophantine equations, and figured out how to find all solutions to such an equation, proving that we can obtain all solutions using our method. First, we use the Euclidean algorithm to find one solution, and then build all other solutions (infinitely many!) by building them from this, and all solutions to a homogeneous linear Diophantine equation.

Date. Thursday, September 10

Notices.

- On Tuesday, I originally mismatched the date/day of the week in the announced deadline for the second investigation module, so we pushed the deadline to 5 pm next Wednesday (September 16).
- We will have an in-person lecture on Tuesday, September 15.

Tasks.

Videos ⟶ Watch the following instructional videos on our new material. Note that we are "skipping" the topics on your current Investigation Module, but we will review them next week.

(1) More on divisibility and greatest common divisors
(2) Bézout's theorem

Investigation module ⟶ Our Euclidean Algorithm Investigation Module is due at 5 pm next Wednesday (September 16). Please see the submission instructions from our digest entry from August 27 if you need a reminder.

Quiz ⟶ Please complete Quiz 2 during your regularly-scheduled class time. It should take about 25 minutes to complete. For instruction details, see the digest entry from September 3.

Office hours ⟶ We will have Office hours from 4–5 pm today. Next week, our office hours will be from 3–4 pm on Monday and 10–11 am on Wednesday. Please check the course website for details.

Problems ⟶ Chapter 3, #27, 28, 40, 43, 44

Reading ⟶ Before next time, read Sections 3D and 3E in your textbook.

Synopsis. During this session, we gained more familiarity with greatest common divisors, and divisibility in general, by investigating and proving several statements. Then we introduced Bézout's theorem, and saw how useful it is. In your second Investigation Module, you will figure out how to build pairs of solutions to the identity in Bézout's theorem.

Date. Tuesday, September 8

Notices. Our session on Thursday will be fully online. Stay safe!

Tasks.

Videos ⟶ Check out the first video, to prepare for Thursday's quiz. If you weren't in class today (of want to go over the material again), watch the other two videos:

(1) Quiz 1 mistakes and solutions
(2) The Division Algorithm
(3) Greatest common divisors

Investigation module ⟶ In our second Investigation Module, you will discover the Euclidean Algorithm, which is essential throughout MATH 558; it will be posted here later today. The module is due at 5 pm next Wednesday (September 16). Please schedule your first team Zoom meeting by Thursday (maybe during the second half of our class period). Make sure to switch roles among yourselves.

Quiz ⟶ We will have a (remote) quiz during our regularly-scheduled time on Thursday; it should take about 25 minutes to complete. You will be asked to prove a statement about infinitely many integers using the Principle of Mathematical Induction. Please do not discuss the quiz problems with your classmates until after the class period. Make sure to review video (1) above to accurately state an inductive hypothesis!

Office hours ⟶ Our Office Hours this week will run from 12–1 pm on Wednesday, and from 4–5 pm on Thursday. Zoom details will be posted on the course website. Please send me an email if you have preferred times for office hours next week!

Problems ⟶ Chapter 3, #4, 5*, 23, 26

*Here, we should have $J = \{e \in \mathbb{Z}, e \geq 1 \mid e = ar + bs \text{ for some } r, s \in \mathbb{Z}\}$.

Reading ⟶ Before next time, read Sections 3B and 3C in your textbook.

Synopsis. Today, we described, investigated, and proved the Division Algorithm, which formalizes the division of one integer by another, with remainder. We also discussed greatest common divisors in more detail, proving a few statements about them.

Date. Thursday, September 3

Notices.

- We will hold an in-person lecture on Tuesday. As usual, the material will be available here as well if you are unable to attend, or prefer not to.
- According to KU IT, MediaHub is now stable! Check out the videos linked below if you haven't yet.

Tasks.

Quiz ⟶ Please read the instructions for completing and submitting Quiz 1, which should be **submitted during your regularly-scheduled class period today**.

- Instructions for completing and submitting quizzes
- Quiz 1

Videos ⟶ Watch the following instructional videos on KU Mediahub:

(1) The Well-ordering Principle
(2) Intro to divisibility
(3) Proving statements via the Well-ordering Principle

Investigation module ⟶ Remember that our first Investigation Module is due tomorrow at 5 pm. The module, and its instructions, are posted in the Course Digest entry from last Thursday.

Office hours ⟶ I will have office hours from 1–2 pm today. Check the Announcements section for the Zoom info. If your Investigation Module team has questions, please try to have at least two members of your group present.

Please send me an email if you have requests on convenient times for office hours next week! They will be posted on Monday.

Problems ⟶ Chapter 2, #32, 34, 35

Reading ⟶ Before next time, read Section 3A in your textbook.

Synopsis. During this session, we study the Well-ordering Principle, which says that every nonempty subset of natural numbers has a least element; this principle is equivalent to the Principle of Mathematical Induction. In fact, it is also equivalent to the Principle of Infinite descent, which states that there is no infinite descending chain of natural numbers. We introduce the notion of divisibility in precise mathematical language, and used the Well-ordering Principle to prove some fundamental properties on this topic.

Date. Tuesday, September 1

Notices. Our next class session, on Thursday, will also be hosted (only) online. Note that there will be a Quiz during class next time; instructions will be detailed then.

Tasks.

Videos ⟶ Watch the instructional videos on the following, posted on KU MediaHub, linked below:

(1) Proving a divisibility property via induction
(2) Intro to complete induction
(3) Proving divisibility by a prime via complete induction
(4) Proving a property about a sequence via complete induction
(5) The equivalence of induction and complete induction

Investigation module ⟶ Meet with your team during class today, and set up subsequent meeting(s) later this week. The module is due on Friday at 5 pm. See the instructions posted last Thursday for details.

Office hours ⟶ We will have office hours again from 1–2 pm on Thursday. Check the Announcements section on the course website for info on how to join. If your Investigation Module team has questions, please try to have at least two members of your group present.

Problems ⟶ Chapter 2, #14, 26, 30, 31

Reading ⟶ Before next time, read Section 2C in your textbook.

Synopsis. This session, we gave an additional example of proving a statement using the Principle of Mathematical Induction (PMI), this time a statement about divisibility. Our main goal after this is to become oriented with the Principle of **Complete** Induction (PCI), apply it in different contexts, and show that it is mathematically "equivalent" to the PMI in the sense that a property can be proved via PMI if and only if it can be proved via PCI.

Date. Thursday, August 27

Notices. Our next class session, on Tuesday, will be hosted (only) online. As mentioned, we will not have live or recorded lectures, but you will be supplied with instructional tools to work through the material (like the videos linked below).

Tasks.

Videos ⟶ If you weren't present in class today, or if you want to review the material, watch the instructional videos on the following, posted on KU Mediahub, linked below:

(1) Some mathematical notation
(2) Intro to mathematical induction
(3) Proving an inequality via induction
(4) Proving a geometric property via induction

Investigation module ⟶ You should soon receive an email with your team assignment for your first investigation module. Please set up your first team Zoom meeting during our regularly-schedule class time period (11 am–12:15 pm or 1–2:15 pm, depending on your section) on Tuesday, September 1. Your team will likely meet multiple times to complete the assignment, so make sure to schedule a follow-up meeting as well. Please read the instructions carefully prior to your Tuesday meeting:

- Instructions for investigation modules
- Module on mathematical induction

The module is due next Friday, September 4, at 5 pm, to be submitted via Blackboard (see the Instructions above). Have fun!

Office hours ⟶ This week, our Office Hours will run from 10–11 am on Tuesday, and 1–2 pm on Thursday. Check the Announcements section on the course website for info on how to join. If your Investigation Module team has questions, please try to have at least two members of your group present.

Reading ⟶ Before next time, read Section 2B in your textbook.

Synopsis. The goals of this class session are to motivate the Principle of Mathematical Induction, state it precisely, and then apply it to prove several very different mathematical properties, but each for all integers larger than a fixed one.

Date. Tuesday, August 25

Notices. Our lecture will be held in person on Thursday. I look forward to seeing some of you then.

Tasks.

Reading ⟶ Carefully review the syllabus and introductory slides.

Problems ⟶ For the following statements $P(n)$ about an integer n, decide whether $P(1), P(2), \ldots, P(5)$ are true. If these are true, do you think that the statement is true for all integers $n \geq 1$?

(1) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$
(2) $n! < n^2$
(3) $n^3 - 5 \leq n^2$
(4) $(n+3) > 2^{n+3}$

Introductory email ⟶ Please send me an email before your regularly-scheduled Thursday class time including the following:

- Your mathematical background (e.g., your completed KU courses), and your general attitude toward math.
- Why you are taking our course, and your future goals.
- Your physical location (e.g., whether you are in Lawrence).
- Whether you have any personal circumstances that might affect your performance in our course.
- If you feel comfortable doing so, I would also appreciate:
  - What is important to you outside of academics. (During class, I shared that I love running with my dogs. I also enjoy fixing things, art museums, and lifting weights with other professors.)
  - A photo of you (without a mask, please). (There is one of me on the front page of my website.)
- Please adhere to our *email etiquette*; in particular, use subject: `[math-558] Introductory email`

Reading ⟶ Before next time, read Section 2A in your textbook.

Synopsis. Today, I introduced myself, and we reviewed the course expectations and guidelines. Next, we detailed the syllabus, and viewed the course website. Finally, we discussed some mathematical notation, and what it means for a statement about an integer to be true. This motivated the question of how we can show that a statement is true for *infinitely* many integers.