

# Midterm topics:

- Truth tables! Practice proving expressions involving  $A, B, \wedge, \vee, \Leftrightarrow, \Rightarrow, \neg$
- Practice proving these expressions **without** truth tables (remember all the laws and theorems)
- Practice dealing with complicated **nested** quantifiers:  $\exists, \forall$  and  $\forall, \exists$ 
  - When can you switch them? When can you not? How do you negate them? Converse? Contrapositive?
  - Look at your Mobius quizzes! Practice working with **complicated** sentences containing  $\forall, \exists$
- Sets! Given  $A$  and  $B$  defined using set builder notation, prove that  $A \subseteq B, A \cap B, A - B = \emptyset$ , etc.
- Look over assignments! Proofs like, if  $A$  then  $B \vee C$ . How do you prove something like that?
- IFF proofs (prove both directions)
- Binomial Theorem! Formula will be given, but make sure you're comfortable with using it!
- Strong induction involving sequences. Practice!
- Proofs involving divisibility
- Polynomials! Divisibility involving polynomials. Roots of polynomials. At least 1 question!

# Midterm tips!

- Use the entire time, please!
  - I used to give 0 to anyone that submitted exam with time still remaining
  - ...unless they got perfect
- Glance through entire midterm before you start it. Make yourself **aware** of what's coming up!
- Get all the “mechanical” questions done.
  - Truth tables,
  - Logical equivalence proofs
  - Relatively easy divisibility proofs,
  - Relatively easy induction proofs,
  - Relatively easy binomial theorem proofs (e.g. manipulating expressions in sum notation to get desired result)
  - T/F questions
    - some *might* be hard. Be careful, but **if something starts taking long, switch to a different question, then come back!**
  - Mark pages that you're complete (checkmark in corner), and ones where you have to come back
- Proofs: it might not be obvious where to begin (for some of them). Give yourself 1 hour for proofs!
- Guide. If 10 questions (4 hard proofs and 6 mechanical/easy proofs like induction that follows the usual pattern): Spend 40 minutes on the 6 “easy” questions, 1 hour on 4 “hard” questions, 10 minutes double-checking solutions, or going back to mechanical questions if proofs were easy, or more time on proofs.
- **Go to the midterm room earlier in the day so you know where it is! Some of you are in a diff. building!**
- **Bring enough lead, or sharpened-pencils, erasers, etc. !!!**

# ~~Winter~~ midterm is coming, what should I do?

[Table of Contents](#) › [Assessments](#) › Extra Practice Problems

## Extra Practice Problems ▾

### Extra Practice Problems

For each *chapter* in the PDF course notes there are extra practice problems. The complete list of practice problems from chapters

- [Extra Practice for Chapter 1](#)
- [Extra Practice for Chapter 2](#)
- [Extra Practice for Chapter 3](#)
- [Extra Practice for Chapter 4](#)
- [Extra Practice for Chapter 5](#)

Bauman, Shane ▾


 Print  Settings

Add dates and restrictions...

Add a description...

Upload / Create ▾

Existing Activities ▾

 Bulk Edit

Expand All || Collapse All

Office hours and YouTube Channel ▾

 Web Page

✓

MATH135F21BaumanMidtermProofPractice ▾

 PDF document

✓

MATH135F21BaumanMidtermProofPracticeSo ▾

 PDF document

✓

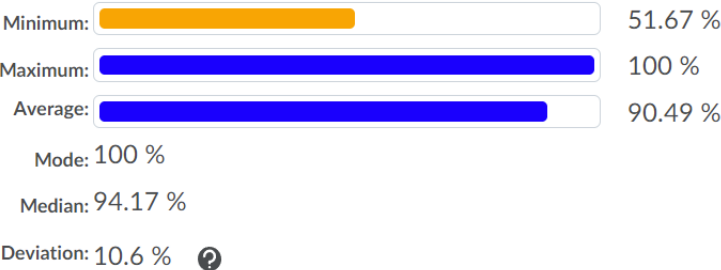
# MATH 135: Lecture 14

Dr. Nike Dattani

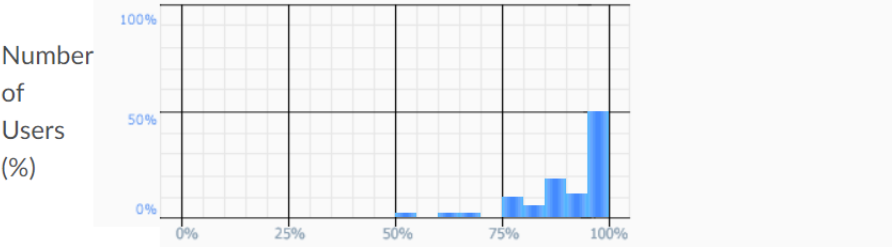
8 October 2021

# Nike's Section 19

Number of submitted grades: 54 / 55

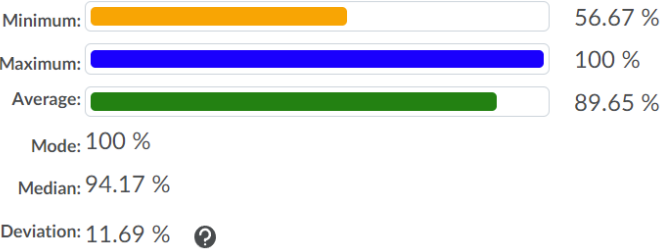


## Grade Distribution

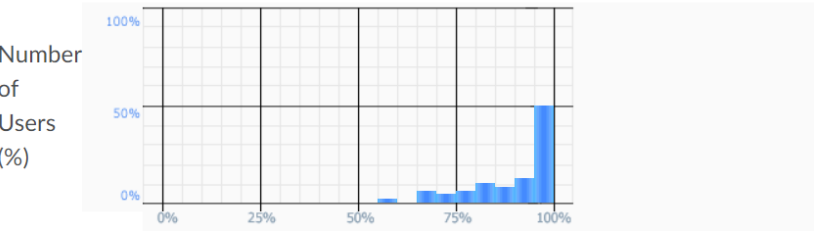


# Nike's Section 16

Number of submitted grades: 48 / 50

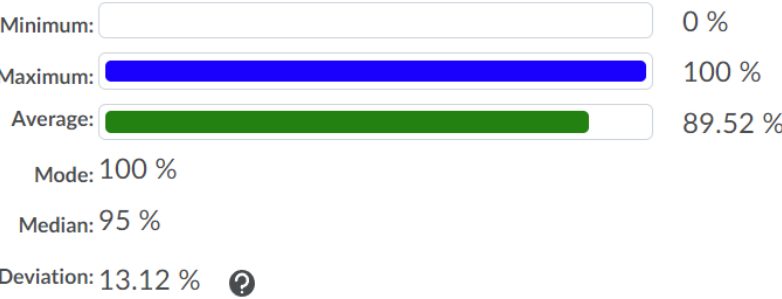


## Grade Distribution

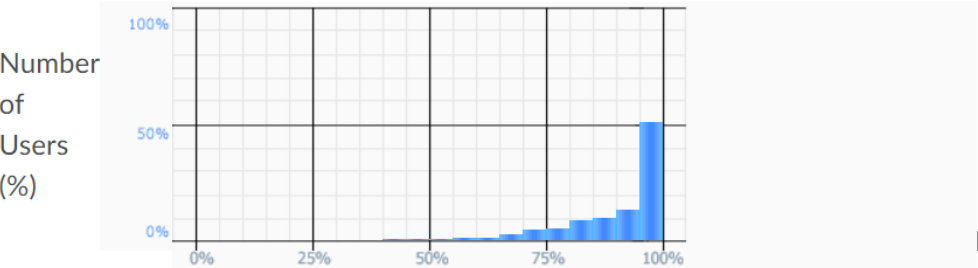


# Entire MATH 135

Number of submitted grades: 1,154 / 1,258



## Grade Distribution



<p><b>MIDTERM</b></p> <p>The midterm will be held <i>in person</i> on Mon Oct 18 from 7 PM to 9 PM EDT</p> <p><a href="#">Mobius Quizzes 13, 14</a></p> <p><b>Available:</b> Wed Oct 20, Fri Oct 22</p> <p><b>Due:</b> midnight</p>	<p><b>Midterm:</b></p> <p>30%</p>	<p>Midterm covers the material from Weeks 1–5</p> <p>Notice that there is no Mobius Quiz on Mon Oct 18</p>
---	-----------------------------------	--

Weeks 1-5. So ignore any practice midterm questions that talk about gcd, mod, etc.

Family Name: \_\_\_\_\_

Given Name: \_\_\_\_\_

Id. No.: \_\_\_\_\_

**Math 135**  
**Algebra for Honours Mathematics**  
**Mid-Term Examination**

2006-06-05 7:00-9:00

**Instructor: B. Tasic**

(b) Prove that the number of primes is infinite.

Euclid's proof (Proposition 20 in Book 9 of *The Elements*):

Assume there's only a finite set of primes, ordered from smallest to largest:  $F = \{ p_1, p_2, \dots, p_n \}$

Let  $P = p_1 p_2 \dots p_n$  (product of all primes).

Let  $Q = P + 1$ .

**Case 1:**  $Q$  is prime. Then  $F$  does not contain all primes, because  $Q > p_n$  and  $Q$  is prime.

**Case 2:**  $Q$  is not prime,

so it contains some prime factor  $r$  such that  $r \mid Q$ , where  $r \neq Q$  and  $r \neq 1$  (i.e.  $1 < r < Q$ )

Then  $r \mid Q$  and  $Q = P + 1$ , so  $r \mid P + 1$

Also,  $r < Q$ , so  $r \leq Q - 1$ , so  $r \leq P$ .

If  $r$  is in the set  $F$ , then  $r \mid P$ .

$r \mid P$ , and  $r \mid P + 1$ , so  $r \mid Px + (P + 1)y$  (D.I.C.)

$r \mid P$ , and  $r \mid P + 1$ , so  $r \mid P + 1 - P$  ( $y = 1, x = -1$ )

$r \mid 1$  (the only number that divides 1 is 1, so  $r \notin F$ )

So for any finite set  $F$  of primes, there's at least one prime missing (either  $Q$ , as in **Case 1**, or  $r$  as in **Case 2**).

\*Note: This is the idea behind Euclid's proof, but unfortunately modern notation wasn't invented yet, so it was less elegant.



## Book IX

### Proposition 20

*Prime numbers are more than any assigned multitude of prime numbers.*

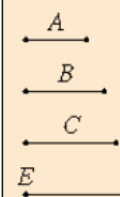
Let  $A$ ,  $B$ , and  $C$  be the assigned prime numbers.

I say that there are more prime numbers than  $A$ ,  $B$ , and  $C$ .

Take the least number  $DE$  measured by  $A$ ,  $B$ , and  $C$ . Add the unit  $DF$  to  $DE$ .

Then  $EF$  is either prime or not.

First, let it be prime. Then the prime numbers  $A$ ,  $B$ ,  $C$ , and  $EF$  have been found which are more than  $A$ ,  $B$ , and  $C$ .



Next, let  $EF$  not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number  $G$ .

I say that  $G$  is not the same with any of the numbers  $A$ ,  $B$ , and  $C$ .

If possible, let it be so. Now  $A$ ,  $B$ , and  $C$  measure  $DE$ , therefore  $G$  also measures  $DE$ . But it also measures  $EF$ . Therefore  $G$ , being a number, measures the remainder, the unit  $DF$ , which is absurd.

Therefore  $G$  is not the same with any one of the numbers  $A$ ,  $B$ , and  $C$ . And by hypothesis it is prime. Therefore the prime numbers  $A$ ,  $B$ ,  $C$ , and  $G$  have been found which are more than the assigned multitude of  $A$ ,  $B$ , and  $C$ .

Therefore, *prime numbers are more than any assigned multitude of prime numbers.*

[VII.31](#)

Q.E.D.

## Guide

This proposition states that there are more than any finite number of prime numbers, that is to say, there are infinitely many primes.

### Outline of the proof

Suppose that there are  $n$  primes,  $a_1, a_2, \dots, a_n$ . Euclid, as usual, takes an specific small number,  $n = 3$ , of primes to illustrate the general case. Let  $m$  be the least common multiple of all of them. (This least common multiple was also considered in proposition [IX.14](#). It wasn't noted in the proof of that proposition that the least common multiple of primes is their product, and it isn't noted in this proof, either.)

Consider the number  $m + 1$ . If it's prime, then there are at least  $n + 1$  primes.

So suppose  $m + 1$  is not prime. Then according to [VII.31](#), some prime  $g$  divides it. But  $g$  cannot be any of the primes  $a_1, a_2, \dots, a_n$ , since they all divide  $m$  and do not divide  $m + 1$ . Therefore, there are at least  $n + 1$  primes. Q.E.D.

This proposition is not used in the rest of the *Elements*.

6. (a) Let  $a$  and  $b$  be integers. Prove that  $a^3|b^3$  if and only if  $a|b$

$$a \mid b \Rightarrow a^3 \mid b^3$$

$$b = k a, \text{ so } b^3 = k^3 a^3$$

$k^3$  is an integer, so  $a^3 \mid b^3$  with  $k^3$  the constant.

$$a^3 \mid b^3 \Rightarrow a \mid b$$

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \quad b = p_1^{\beta_1} \cdots p_r^{\beta_r}$$

where  $\alpha_i, \beta_i \geq 0$ . Allow the exponents to possibly be 0 if such a prime  $p_i$  occurs in the factorization of one integer but not the other.

So  $a^2 = p_1^{2\alpha_1} \cdots p_r^{2\alpha_r}$  and  $b^2 = p_1^{2\beta_1} \cdots p_r^{2\beta_r}$ . Since  $a^2 \mid b^2$ , by unique factorization, necessarily  $2\alpha_i \leq 2\beta_i$  for each  $i$ . That implies  $\alpha_i \leq \beta_i$  for all  $i$ , and so  $a \mid b$ .

About 2,710,000 results (0.67 seconds)

The Infinity of Primes. The number of primes **is infinite**. The first ones are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 and so on. The first proof of this important theorem was provided by the ancient Greek mathematician Euclid. Aug. 3, 2020

<https://towardsdatascience.com/proving-the-infinity-of-p...>

### Proving the Infinitude of Primes Using Elementary Calculus

[About featured snippets](#)
[Feedback](#)

### People also ask

How do you prove there is an infinite number of primes?



Who proved that there are an infinite number of prime numbers?



Are prime numbers infinite or finite?



How do you prove by contradiction there are infinite prime numbers?


[Feedback](#)
[https://en.wikipedia.org/wiki/Euclid's\\_theorem](https://en.wikipedia.org/wiki/Euclid's_theorem)

### Euclid's theorem - Wikipedia

Euclid's theorem is a fundamental statement in number theory that asserts that there are **infinitely many prime numbers**. It was first proved by Euclid in his ...

[Euclid's proof](#) · [Euler's proof](#) · [Erdős's proof](#) · [Some recent proofs](#)

# Euclid's theorem

From Wikipedia, the free encyclopedia

*This article is about the theorem on the infinitude of prime numbers. For the theorem on perfect numbers and Mersenne primes, see [Euclid–Euler theorem](#).*

**Euclid's theorem** is a fundamental statement in [number theory](#) that asserts that there are [infinitely](#) many [prime](#) numbers. It was first proved by Euclid.

## Contents [hide]

- [Euclid's proof](#)
  - [Variations](#)
- [Euler's proof](#)
- [Erdős's proof](#)
- [Furstenberg's proof](#)
- [Some recent proofs](#)
  - [Proof using the inclusion-exclusion principle](#)
  - [Proof using de Polignac's formula](#)
  - [Proof by construction](#)
  - [Proof using the irrationality of  \$\pi\$](#)
  - [Proof using information theory](#)
- [Stronger results](#)
  - [Dirichlet's theorem on arithmetic progressions](#)
  - [Prime number theorem](#)
  - [Bertrand–Chebyshev theorem](#)
- [Notes and references](#)
- [External links](#)

## Euclid's proof [\[ edit \]](#)

Euclid offered a proof published in his work *Elements* (Book IX, Proposition 20),<sup>[1]</sup> which is paraphrased here.<sup>[2]</sup>

Consider any finite list of prime numbers  $p_1, p_2, \dots, p_n$ . It will be shown that at least one additional prime number not in this list exists. Let  $P$  be the product of all the primes in the list. Then  $q$  is either prime or not:

- If  $q$  is prime, then there is at least one more prime that is not in the list, namely,  $q$  itself.



a^2 divides b^2 implies a divides b



All



Images



News



Videos



Shopping



More

About 19,600,000 results (0.56 seconds)

https://math.stackexchange.com › questions › if-a2-divi...

If  $a^2$  divides  $b^2$ , then  $a$  divides  $b$  - Math Stack ...

To say that  $a^2$  divides  $b^2$  is to say that  $n = b^2/a^2 = (b/a)^2$  is an integer. Now integers only have



MATHEMATICS

Home

PUBLIC

Questions

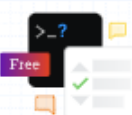
Tags

Users

Unanswered

TEAMS

Stack Overflow for Teams – Collaborate and share knowledge with a private group.



Create a free Team

What is Teams?

## If $a^2$ divides $b^2$ , then $a$ divides $b$ [duplicate]

Asked 9 years, 1 month ago · Active 9 months ago · Viewed 45k times

This question already has answers here:

[Show that  \$a^n \mid b^n\$  implies  \$a \mid b\$](#)  (4 answers)

[How to prove: if  \$a, b \in \mathbb{N}\$ , then  \$a^{1/4}\$  is an integer or an irrational number?](#) (43 answers)

Closed 10 months ago.

Let  $a$  and  $b$  be positive integers. Prove that: If  $a^2$  divides  $b^2$ , then  $a$  divides  $b$ .

Context: the lecturer wrote this up in my notes without proving it, but I can't seem to figure out why it's true. Would appreciate a solution.

elementary-number-theory divisibility

Share Cite Follow

edited Aug 15 '12 at 20:27



user2468

asked Aug 15 '12 at 20:15



confused

539 ● 1 ● 6 ▲ 10

3 Do you have the fundamental theorem of arithmetic at your disposal? – [yunone](#) Aug 15 '12 at 20:18

Yep! We covered that a couple weeks ago. – [confused](#) Aug 15 '12 at 20:20

2 Hint: if  $a^2 \mid b^2$  then  $b^2 = ?$  and  $?$  is a perfect square so ... – [Mark Bennet](#) Aug 15 '12 at 20:22

3 Hint: If  $b^2 = ka^2$  then using FTA what can you say about  $k$ ? Perfect square. Why? Something about the even powers of primes. – [user2468](#) Aug 15 '12 at 20:25

2 There are many prior answers on the irrationality of square roots, e.g. see [here](#) and [here](#) and [here](#). – [Bill Dubuque](#) Aug 15 '12 at 21:53

Show 6 more comments

8 Answers

Active

Oldest

Votes

By the fundamental theorem of arithmetic, you can write  $a$  and  $b$  as a product of primes, say

64

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \quad b = p_1^{\beta_1} \cdots p_r^{\beta_r}$$

where  $\alpha_i, \beta_i \geq 0$ . Allow the exponents to possibly be 0 if such a prime  $p_i$  occurs in the factorization of one integer but not the other.

So  $a^2 = p_1^{2\alpha_1} \cdots p_r^{2\alpha_r}$  and  $b^2 = p_1^{2\beta_1} \cdots p_r^{2\beta_r}$ . Since  $a^2 \mid b^2$ , by unique factorization, necessarily  $2\alpha_i \leq 2\beta_i$  for each  $i$ . That implies  $\alpha_i \leq \beta_i$  for all  $i$ , and so  $a \mid b$ .

Share Cite Follow

edited Aug 15 '12 at 21:23

answered Aug 15 '12 at 20:29



yunone

21.2k ● 7 ● 71 ▲ 151



Name (Print):

UW Student ID Number:

**University of Waterloo**  
**First Midterm Test**  
**Math 135**  
(Algebra for Honours Mathematics)

**Instructor:** R.D. Willard

**Date:** Monday, February 6, 2006

**Term:** 1061

**Number of pages:** 7  
(including cover page)

**Section:** 001

**Time:** 7:15 p.m. to 8:30 p.m.

**Duration of test:** 75 minutes

**Test type:** closed book

# Good luck on midterm !!!

Thank you so much for paying attention so far!