

From Faculty Member to OER Advocate: Reflections on Two Journeys

Emily Ragan ([Metropolitan State University of Denver](#))
Jonathan Poritz ([Colorado State University-Pueblo](#))

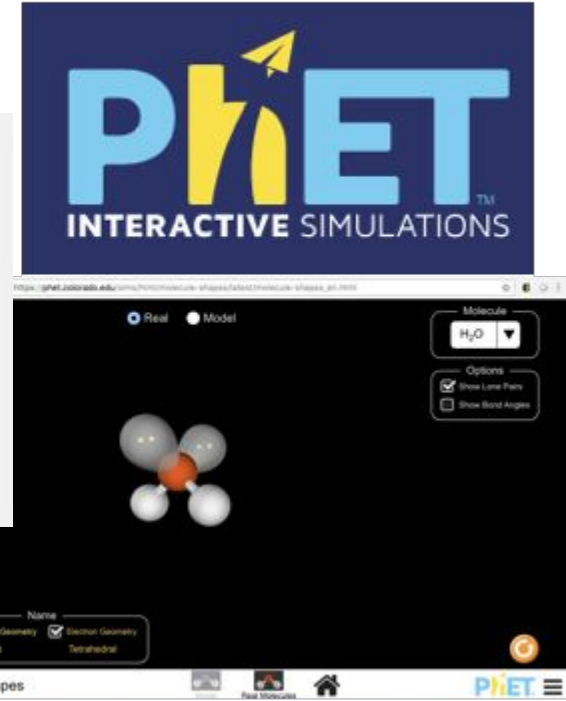
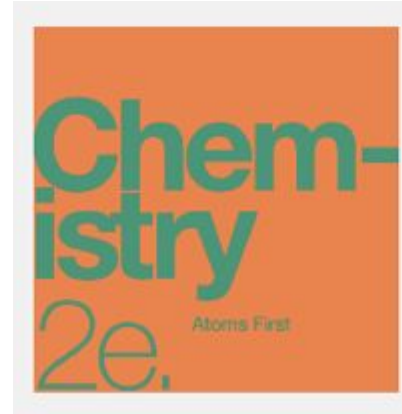


This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](#).

Emily's path to OER use and advocacy



The importance of focusing on
learning objectives first,
resources second



DIY Online Homework System

- Created my own online homework/quiz/exam system in our LMS (Blackboard)
- Advantages:
 - Gave me a lot of control over content and alignment of questions with my learning objectives
 - No additional cost to students
 - No additional system to navigate
- Disadvantages:
 - Took a lot of time
 - Requires troubleshooting
 - Giving adequate feedback is hard



Active learning



Creating and sharing an innovative module in Biochemistry II

- <https://serc.carleton.edu/curenet/index.html>

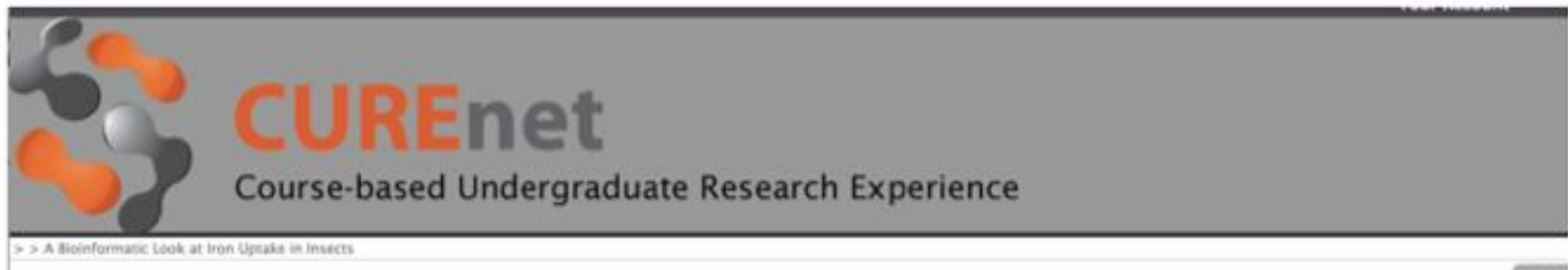
CUREs



CURE Collection »

Course-based Undergraduate Research Experiences (CUREs)

- Students engage in research during a course so that more students have exposure to research experiences
- The work must be on a real scientific problem with the potential to make discoveries that are of interest to the scientific community
- Progress is iterative, involving repetition and trouble-shooting
- The results are communicated back to stakeholders



Student Goals

1. Use common database and bioinformatics tools to explore a gene and analyze protein sequences
2. Analyze data and generate novel predictions; make and defend the structure/function-related conclusions drawn from data
3. Communicate about research progress, including keeping quality records during the process

Research Goals

1. Investigate proteins involved in *Drosophila* iron uptake and find potential orthologs other insect species.
2. Make a multiple sequence alignment of the assigned *Drosophila* protein and related insect proteins, then use the alignment and protein family information or a related crystal structure to identify key amino acid residues and make predictions about protein structure and function

Instructional Materials

Schedule for CHE 4320 and Iron-uptake CURE (Microsoft Word 2007 (.docx) 139kB May3 19)

Benching Introductory User Guide for CHE 4320.docx (Microsoft Word 2007 (.docx) 79kB May2 19)

Directions for Benchling Posts (Microsoft Word 2007 (.docx) 154kB May1 19)

Day 2 CHE 4320 Spring 2019 Group 1.docx (Microsoft Word 2007 (.docx) 84kB May3 19)

Day 3 of Class & Group project Day 2 Sp 2019.docx (Microsoft Word 2007 (.docx) 68kB May3 19)

Day 4 Day 3 of project Transcripts S19.docx (Microsoft Word 2007 (.docx) 74kB May3 19)

Day 5 Analyzing RNA Seq data CHE 4320 Spring 2019 .docx (Microsoft Word 2007 (.docx) 1.4MB May3 19)

Day 7 Protein alignment Sp19.docx (Microsoft Word 2007 (.docx) 355kB May3 19)

Day 8 Chimera 3D structure.docx (Microsoft Word 2007 (.docx) 280kB May3 19)

Group Evaluation for DNA protein project.docx (Microsoft Word 2007 (.docx) 73kB May1 19)

Assessment

Benchling Entry Rubric (Microsoft Word 2007 (.docx) 66kB Jun6 18)

Instructions for the Memo to Maureen.docx (Microsoft Word 2007 (.docx) 160kB May2 19)

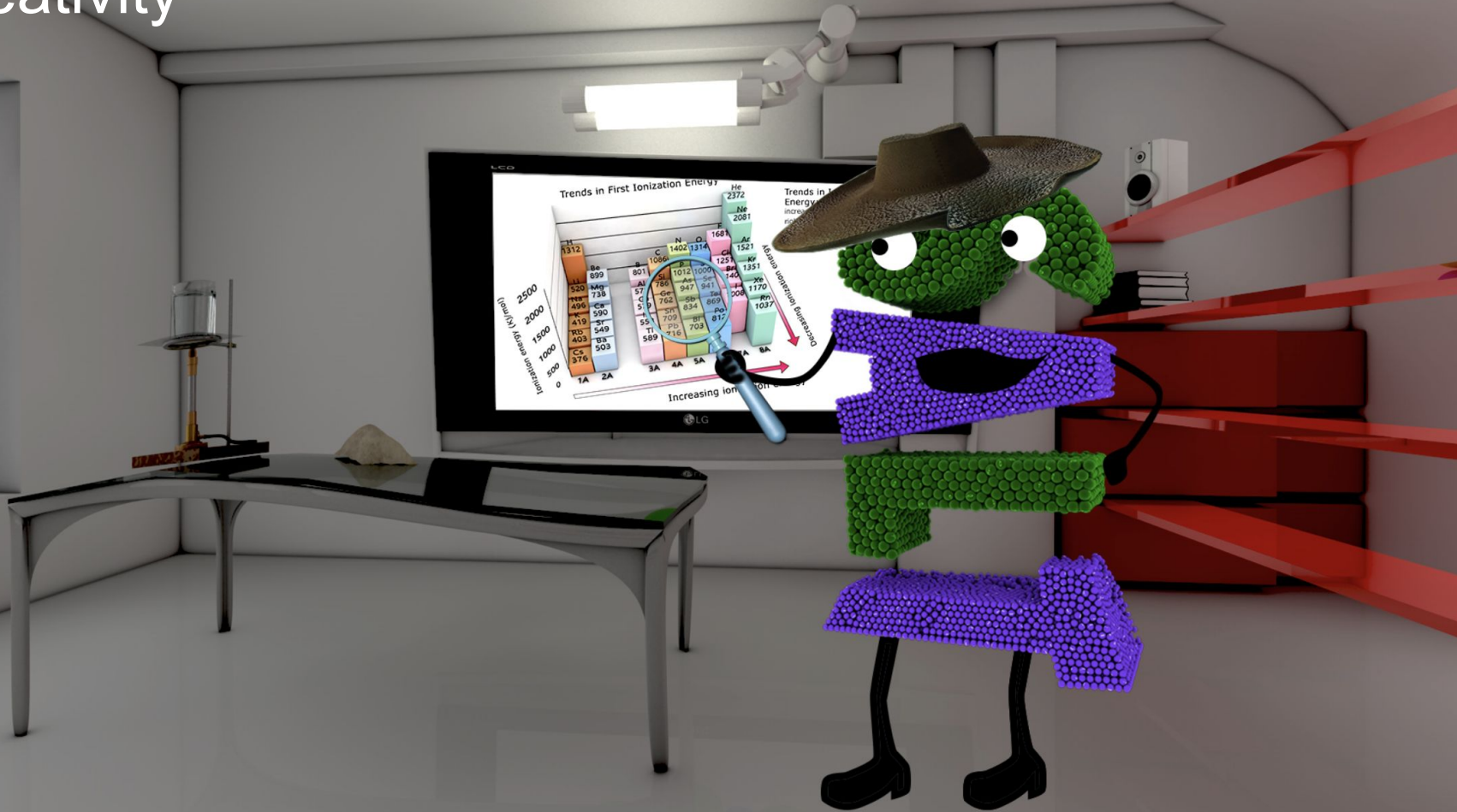
This item is offered under a Creative Commons Attribution-NonCommercial-ShareAlike license

<http://creativecommons.org/licenses/by-nc-sa/3.0/> You may reuse this item for non-commercial purposes as long as you provide attribution and offer any derivative works under a similar license.

Agency



Creativity



Recall + Reflection = Lasting Learning

↕ ↕
Content



When I share with fellow faculty,

- Identify challenges we face in our courses
- Invite a discussion about how resources (textbooks, etc.) help with the challenges
- Discuss learning strategies that may not be supported by our resources



Jonathan's path to OER use and advocacy

1. **CSU-Pueblo Math 419**, *Number Theory*, spring 2012: Student-written textbook, using MediaWiki & MathJax, because of poor departmental scheduling.
2. **CSU-Pueblo Math 242**, *MATLAB Computation*, spring 2014: Students use Linux, Octave, other FLOSS tools, because they're just better; early JITERs.
3. **CSU-Pueblo Math 319**, *Number Theory*, spring 2014: OER creation ["YAINTT"], usually a week ahead of the class, because how hard could it be?
4. **CSU-Pueblo Math 319**, *Number Theory*, spring 2015: OER creation ["YAINTT, v2.0"], because this should just be polishing by now, right?
5. **CSU-Pueblo Math 411**, *Introduction to Topology*, summer 2015: use and some creation of OER, because this is in my blood, I'm not giving up control to a textbook.
6. **CSU-Pueblo Math 156**, *Introduction to Statistics*, Fall 2016 (one online, one in-person): use of existing OER with my supplements, because of the cost of the commercial book.
7. **Reykjavík U. T-[7,8]50-CYCR**, *Cryptocurrencies*, Winter 2016: full-on JITER creation.
8. **CSU-Pueblo Math 156**, *Introduction to Statistics*, Spring 2017 (two sections): OER creation ["LDLoS"], because this must just be polishing, this time, right?

CSUP Math 419, *Number Theory*, Spring 2012

I was assigned to this quite advanced class [but required of teacher-ed math majors!] at the last minute. The bookstore had already ordered, and some (but not all) students had purchased *A Friendly Introduction to Number Theory*, by Joseph H. Silverman -- a perfectly nice book. But it cost around \$180, the first two chapters are available on the author's website, and I didn't want to cover much in later chapters.

So I spun up a [MediaWiki](#) instance on my website -- poritz.net/jonathan; it helps to own your own name on the Internet -- and assigned the students in rotating, carefully chosen pairs, to take notes each week and to write them up on that wiki.

What is MediaWiki?

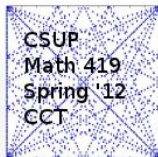
It's the FLOSS[="Free/libre/open-source software"]
behind the 8th most popular
website on the planet.

Administering it was of
moderate difficulty in 2012,
but today [e.g., on the site
reclaimhosting.com] is
mostly just point-and-click.



Front page of

Math 419 Class Collaborative Textbook



[Main page](#)
[HW/schedule](#)
[Syllabus/policies](#)
[Recent changes](#)
[wikitext help](#)
[TeX help](#)

Tools

[What links here](#)
[Related changes](#)
[Special pages](#)
[Printable version](#)
[Permanent link](#)
[Page information](#)

[Kaleb](#) [Talk](#) [Preferences](#) [Watchlist](#) [Contributions](#) [Log out](#)

[Main page](#)

[Discussion](#)

[Read](#)

[Edit](#)

[View history](#)



[More](#) ▾



Main Page

CSU-P Math 419 Class Wiki [\[edit\]](#)

This is the class wiki for **Math 419: Number Theory** at Colorado State University -- Pueblo, in the Spring of 2012.

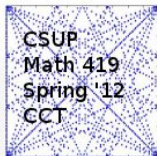
Please edit the [General Discussion](#) page and simply add your comments or questions to the end, if there are any things you are thinking about regarding the material we are working on, or if you have questions about some homework problem, etc.

Class Collaborative Textbook [\[edit\]](#)

In the following, the main chapters are student contributions (of rigor, precision, and formality) to the corresponding chapter of our textbook. The non-integrally numbered chapters are contributions by the instructor to provide some supplementary material which is not simply an expansion of the book chapters.

- [Chapter 1](#): What Is Number Theory?
- [Chapter 2](#): Pythagorean Triples
- [Chapter 3](#): Pythagorean Triples and the Unit Circle
- [Chapter 4](#): Sums of Higher Powers and Fermat's Last Theorem
- [Chapter 5](#): Divisibility and the Greatest Common Divisor
- [Chapter 6](#): Linear Equations and the Greatest Common Divisor
 - [Chapter 6.1](#): Alternate induction
- [Chapter 7](#): Factorization and the Fundamental Theorem of Arithmetic
- [Chapter 8](#): Congruences
 - [Chapter 8.1](#): The Linear Congruence Theorem via Inverses mod n
- [Chapter 9](#): Congruences, Powers, and Fermat's Little Theorem
- [Chapter 10](#): Congruences, Powers, and Euler's Formula
 - [Chapter 10.1](#): Notes on problem 10.1
- [Chapter 11](#): Euler's Phi Function and the Chinese Remainder Theorem
- [Chapter 12](#): Prime Numbers
- [Chapter 13](#): Counting Primes
- [Chapter 14](#): Mersenne Primes
- [Chapter 15](#): Mersenne Primes and Perfect Numbers
- [Chapter 16](#): Powers Modulo m and Successive Squaring

Chapter 10 [by students] of Math 419 Class Collaborative Textbook



[Main page](#)
[HW/schedule](#)
[Syllabus/policies](#)
[Recent changes](#)
[wikitext help](#)
[TeX help](#)

[Tools](#)
[What links here](#)
[Related changes](#)
[Special pages](#)
[Printable version](#)
[Permanent link](#)
[Page information](#)

[Kaleb](#) [Talk](#) [Preferences](#) [Watchlist](#) [Contributions](#) [Log out](#)

Page [Discussion](#)

[Read](#)

[Edit](#)

[View history](#)



[More](#) ▾

Search Class wiki for Poritz's Math 419



Chapter 10

Congruences, Powers, and Euler's Formula [\[edit\]](#)

Theorem 10.1 (Euler's Formula): If $\gcd(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

The function ϕ is called *Euler's phi function*. We can define ϕ as the number of integers between 1 and m that are relatively prime to m , written

$$\phi(m) = \# \{a : 1 \leq a \leq m \text{ and } \gcd(a, m) = 1\}.$$

Contents [\[hide\]](#)

- 1 [Congruences, Powers, and Euler's Formula](#)
 - 1.1 [Note](#)
 - 1.2 [definition](#)

[Continue to Chapter 11](#) (Or visit [A discussion of the surprisingly intricate problem 10.1](#))

Note [\[edit\]](#)

If we want $K^{\phi(m)} \equiv 1 \pmod{m}$

then we need

$$\gcd(K, m) = 1$$

$$K^{\phi(m)} - 1 = lm$$

$$K^{\phi(m)} - lm = 1$$

$$KK^{\phi(m)-1} + m(-l) = 1$$

l is a linear combination of K, m

The $\gcd$ is the smallest possible linear combination of K, m

so the $\gcd(K, m) = 1$

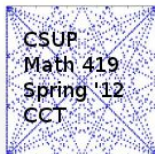
Claim 10.2 If $\gcd(a, m) = 1$ then the numbers

$b_1a, b_2a, \dots, b_{\phi(m)}a \pmod{m}$ are the same as the numbers

$b_1, b_2, \dots, b_{\phi(m)} \pmod{m}$ although they may be in a different order.

Chapter 10.1 [by JP] of

Math 419 Class Collaborative Textbook



[Main page](#)
[HW/schedule](#)
[Syllabus/policies](#)
[Recent changes](#)
[wikitext help](#)
[TeX help](#)

[Tools](#)
[What links here](#)
[Related changes](#)
[Special pages](#)
[Printable version](#)
[Permanent link](#)
[Page information](#)



Chapter 10.1

Notes on problem 10.1 [\[edit\]](#)

Contents [\[hide\]](#)

- 1 Notes on problem 10.1
 - 1.1 The Problem
 - 1.2 What we noticed in class on 7 March 2012
 - 1.3 But unfortunately...
 - 1.4 Some more thoughts
 - 1.5 Looking more closely at $\mathcal{R}_1$

The Problem [\[edit\]](#)

We are supposed to consider the number B as defined in the ourproof of Euler's Formula. So suppose $m \in \mathbb{N}$ has $m > 2$. There are $\phi(m)$ natural numbers less than m which are relatively prime to m (this is the definition of $\phi(m)$!), put them in order and call them $b_1, \dots, b_{\phi(m)}$, so

$$1 = b_1 < \dots < b_{\phi(m)} < m \quad .$$

Define $B = \prod_{j=1}^{\phi(m)} b_j$. We are supposed to show that $B \equiv \pm 1 \pmod m$ and then see if we can characterize the numbers m for which B has each sign.

What we noticed in class on 7 March 2012 [\[edit\]](#)

Let's define a set of natural numbers

$$\mathcal{R} = \{b \in \mathbb{N} \mid \gcd(b, m) = 1\} \quad .$$

As we just said, the number of elements in $\mathcal{R}$ is $\phi(m)$.

But we've met this set $\mathcal{R}$ before: it is exactly the set of elements of $\mathbb{Z}/m$ which are invertible.

But think of some $k \in \mathcal{R}$. It is invertible, so $k^{-1} \pmod m$ exists. But then $(k^{-1})^{-1} \pmod m$ also exists: it's just k . So $k^{-1} \in \mathcal{R}$ as well. Thus inversion is a permutation of $\mathcal{R}$, let's write it as $\iota : \mathcal{R} \rightarrow \mathcal{R}$.

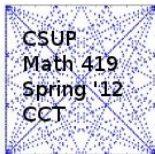
Now think about B^2 . It is the product of all the elements of $\mathcal{R}$, twice, so we can rearrange the terms so that each element in the first B is put next to a unique element from the second B , which is its inverse! Thus $B^2 \equiv 1 \pmod m$.

Certainly ± 1 are solutions to the equation $x^2 \equiv 1 \pmod m$. Wouldn't it be nice if these were the *only* solutions - then we would be done, B would have

Chapter 10.1, editing, of

Math 419 Class Collaborative Textbook

Looks just like
editing
Wikipedia,
obviously.



[Main page](#)
[HW/schedule](#)
[Syllabus/policies](#)
[Recent changes](#)
[wikitext help](#)
[TeX help](#)

[Tools](#)
[What links here](#)
[Related changes](#)
[Special pages](#)
[Page information](#)

[Kaleb Talk](#) [Preferences](#) [Watchlist](#) [Contributions](#) [Log out](#)

Page [Discussion](#)

[Read](#)

[Edit](#)

[View history](#)



[More](#) ▾



Editing Chapter 10.1

=Notes on problem 10.1=

__TOC__

====The Problem====

We are supposed to consider the number B as defined in the ourproof of Euler's Formula. So suppose $m \in \mathbb{N}$ has $m > 2$. There are $\phi(m)$ natural numbers less than m which are relatively prime to m (this is the definition of $\phi(m)$!), put them in order and call them $b_1, \dots, b_{\phi(m)}$, so $1 = b_1 < \dots < b_{\phi(m)} \leq m$. Define $B = \prod_{j=1}^{\phi(m)} b_j$. We are supposed to show that $B \equiv 1 \pmod{m}$ and then see if we can characterize the numbers m for which B has each sign.

====What we noticed in class on 7 March 2012====

Let's define a set of natural numbers $\{\mathcal{R}\} = \{b \in \mathbb{N} \mid \gcd(b, m) = 1\}$. As we just said, the number of elements in $\{\mathcal{R}\}$ is $\phi(m)$.

But we've met this set $\{\mathcal{R}\}$ before: it is exactly the set of elements of $\mathbb{Z}/m\mathbb{Z}$ which are invertible.

But think of some $k \in \{\mathcal{R}\}$. It is invertible, so $k^{-1} \pmod{m}$ exists. But then $\left(k^{-1} \pmod{m}\right)^{-1} \pmod{m}$ also exists: it's just k . So $k^{-1} \in \{\mathcal{R}\}$ as well. Thus inversion is a permutation of $\{\mathcal{R}\}$, let's write it as $\iota: \{\mathcal{R}\} \rightarrow \{\mathcal{R}\}$.

Now think about B^2 . It is the product of all the elements of $\{\mathcal{R}\}$, twice, so we can rearrange the terms so that each element in the first B is put next to a unique element from the second B , which is its inverse! Thus $B^2 \equiv 1 \pmod{m}$.

Certainly ± 1 are solutions to the equation $x^2 \equiv 1 \pmod{m}$. Wouldn't it be nice if these were the 'only' solutions -

Summary:

☐ This is a minor edit ☒ Watch this page

Please note that all contributions to Class wiki for Poritz's Math 419 may be edited, altered, or removed by other contributors. If you do not want your writing to be edited mercilessly, then do not submit it here.

You are also promising us that you wrote this yourself, or copied it from a public domain or similar free resource (see [My wiki:Copyrights](#) for details). **Do not submit copyrighted work without permission!**

[Save changes](#)

[Show preview](#)

[Show changes](#)

[Cancel](#) [Editing help](#) (opens in new window)

Chapter 10.1,
editing,
hacker's view,
of

Math 419
Class
Collaborative
Textbook

Maybe not
exactly like
Wikipedia
editing...
because of
LaTeX

```
emacs
=Notes on problem 10.1=
__TOC__

====The Problem====
We are supposed to consider the number  $B$  as defined in the book's proof of Euler's Formula. So suppose
 $m \in \mathbb{N}$  has  $m \not\equiv 2 \pmod{3}$ . There are  $\phi(m)$  natural numbers less than  $m$  which are relatively prime to
 $m$  (this is the definition of  $\phi(m)$ !), put them in order and call them  $b_1, \dots, b_{\phi(m)}$ , so
 $1 = b_1 \leq \dots \leq b_{\phi(m)} \leq m$ . Define  $B = \prod_{j=1}^{\phi(m)} b_j$ . We are supposed to show that
 $B \equiv 1 \pmod{m}$  and then see if we can characterize the numbers  $m$  for which  $B$  has each sign.

====What we noticed in class on 7 March 2012====
Let's define a set of natural numbers  $\mathcal{R} = \{b \in \mathbb{N} \mid \gcd(b, m) = 1\}$ . As we just said, the
number of elements in  $\mathcal{R}$  is  $\phi(m)$ .

But we've met this set  $\mathcal{R}$  before: it is exactly the set of elements of  $\mathbb{Z}/m\mathbb{Z}$  which are invertible.
But think of some  $k \in \mathcal{R}$ . It is invertible, so  $k^{-1} \pmod{m}$  exists. But then
 $k^{-1} \pmod{m}$  also exists; it's just  $k$ . So  $k^{-1} \in \mathcal{R}$  as well. Thus
inversion is a permutation of  $\mathcal{R}$ , let's write it as  $\iota: \mathcal{R} \rightarrow \mathcal{R}$ .

Now think about  $B^2$ . It is the product of all the elements of  $\mathcal{R}$ , twice, so we can rearrange the
terms so that each element in the first  $B$  is put next to a unique element from the second  $B$ , which is its
inverse! Thus  $B^2 \equiv 1 \pmod{m}$ .

Certainly  $\pm 1$  are solutions to the equation  $x^2 \equiv 1 \pmod{m}$ . Wouldn't it be nice if these were the
"only" solutions - then we would be done,  $B$  would have to be  $\pm 1 \pmod{m}$ .

====But unfortunately...====
This hope is completely misguided: in fact, there are usually many solutions to  $x^2 \equiv 1 \pmod{m}$ , which is
important in the real solution. We actually had many examples on the board in class of other solutions, for many
values of  $m$ .

====Some more thoughts====
We were nevertheless on a very good track in class, and need only be a little bit more careful.

There are two kinds of elements in  $\mathcal{R}$ : those which are moved by the permutation  $\iota$  and those
which are not. The elements which are moved by  $\iota$  are actually moved to some other element, but then another
application of  $\iota$  moves them right back; that is,
 $\forall k \in \mathcal{R}, \iota(\iota(k)) = k$ . In fact, let's say there are  $\phi_1(m)$  elements in the set
 $\mathcal{R}_1 = \{k \in \mathcal{R} \mid \iota(k) = k\}$  and  $\phi_2(m) = \phi(m) - \phi_1(m)$  in the rest of  $\mathcal{R}$ , which remaining part of  $\mathcal{R}$  we
shall write as  $\mathcal{R}_2 = \{k \in \mathcal{R} \mid \iota(k) \neq k\}$ . Now notice that  $\mathcal{R}_2$  consists of pairs of elements, a number  $k$  and its inverse  $\iota(k)$ . It
follows that  $B_2 = \prod_{k \in \mathcal{R}_2} k$  has every element in it multiplied by another element which is its
inverse mod  $m$ , so  $B_2 \equiv 1 \pmod{m}$ .

Therefore  $B = \prod_{k \in \mathcal{R}} k = \prod_{k \in \mathcal{R}_1} k \cdot \prod_{k \in \mathcal{R}_2} k$ 
-:-- Chapter 10.1 Top (20,242) (Nroff Wrap)
```

MediaWiki with MathJax uses both **wikitext** and **LaTeX**, two *markup languages*.

wikitext: to put *something* in italics, do “something”; links are [URL text], *etc.*

There’s not much to it (most common markup fits on a one-page cheat sheet), and wiki editing is a valuable life skill, why not learn it here and now?

LaTeX: for equations, enclose bits of text in \$’s, e.g.: $e^{i\pi} = -1$ makes $e^{i\pi} = -1$

All mathematicians, computer scientists, and physicists use LaTeX, why not learn it here and now?

HTML is also a markup language (HTML=“Hypertext Markup Language”, in fact), so learning wikitext and LaTeX will help build towards web literacy...

My colleagues said the students would never be able to do it, but there was literally not a single complaint from the students about the technology.

CSUP Math 242, *MATLAB Computation*, Spring 2014

Two aspects of this course, the software environment and the text[s], *etc.*, were OER -- remember OER is not all text!

Software: Rather than use the commercial (expensive) MATLAB running on lab Windoze PCs, students booted Linux, a FLOSS operating system, from thumb drives and Octave, a FLOSS alternative [superset] of MATLAB.

A majority of (silicon) CPUs on the planet use Linux and FLOSS, why not learn about them here and now? ..Also, FLOSS is to commercial software exactly as OER are commercial texts, so why *wouldn't* we use FLOSS alternatives?

Text[s]: all OER, of a form I am calling ***JITERs*** [for ***Just-In-Time-Educational-Resources***] ... the subject of another talk here at OpenEd19....

CSUP Math 319, *Number Theory*, Spring 2014

Note the course was demoted in the intervening two years (400→300).

The material was easier, I was used to writing myself detailed class notes, I'm very comfortable in LaTeX, why not put the notes together into chapters? I tried to stay a week ahead of where the students were and usually (mostly?) succeeded.

This turns out to be a lot of work.

But the students appreciated it, and the book **Yet Another Introductory Number Theory Textbook** [YAINTT] had all those famous advantages of OER. Mostly, it covered exactly what I wanted it to cover, how I wanted that covered....

READING TO ACCOMPANY CSU-P MATH 319
NUMBER THEORY
SPRING TERM, 2014

JONATHAN A. PORITZ AFTER WISSAM RAJI

1. WELL-ORDERING AND DIVISION

1.1. The Well-Ordering Principle and Mathematical Induction. In this section, we present three basic tools that will often be used in proving properties of the integers. We start with a very important property of integers called the well-ordering principle. We then state what is known as the pigeonhole principle, and then we proceed to present an important method called mathematical induction.

1.1.1. The Well-Ordering Principle.

Definition 1.1. Given a set S of numbers (of any kind), we say that $\ell \in S$ is a **least element** of S if $\forall x \in S$, either $x = \ell$ or $\ell < x$.

The Well-Ordering Principle. Every non-empty set of natural numbers has a least element.

This principle is often taken as an axiom.

1.1.2. The Pigeonhole Principle.

The Pigeonhole Principle. Let $s, k \in \mathbb{N}$ satisfy $s > k$. If s objects are placed in k boxes, then at least one box contains more than one object.

Date: 17 February 2014 00:51 These notes are adapted by Jonathan Poritz from **An Introductory Course in Elementary Number Theory** by Wissam Raji, see www.saylor.org/books/. Both these notes and Raji's text are released under a Creative Commons CC BY 3.0 license, see

<https://creativecommons.org/licenses/by/3.0/>



READING TO ACCOMPANY CSU-P MATH 319
NUMBER THEORY
SPRING TERM, 2014

JONATHAN A. PORITZ AFTER WISSAM RAJI

2. CONGRUENCES

A congruence is nothing more than a statement about divisibility. The theory of congruences was introduced by Carl Friedrich Gauss, in his monumental *Disquisitiones Arithmeticae* (published in 1801, when he was 24).

We start by introducing congruences and their properties. We then present solutions to linear congruences which will serve as an introduction to the Chinese Remainder Theorem that follows.

2.1. Introduction to congruences. As we mentioned in the introduction, the theory of congruences was developed by Gauss at the beginning of the nineteenth century.

Definition 2.1. Given $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, we say that a is **congruent to b modulo n** if $n \mid (a - b)$, i.e., if $\exists k \in \mathbb{Z}$ such that $a = b + kn$. If a is congruent to b modulo n , we write $a \equiv b \pmod{n}$.

Example 2.2. $19 \equiv 5 \pmod{7}$. Similarly $2k + 1 \equiv 1 \pmod{2}$ which means every odd number is congruent to 1 modulo 2.

Congruence is much like equality in many ways. For example:

Theorem 2.3. Given $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then

(1) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

Date: 17 February 2014 00:51 These notes are adapted by Jonathan Poritz from **An Introductory Course in Elementary Number Theory** by Wissam Raji, see www.saylor.org/books/. Both these notes and Raji's text are released under a Creative Commons CC BY 3.0 license, see

<https://creativecommons.org/licenses/by/3.0/>



READING TO ACCOMPANY CSU-P MATH 319
NUMBER THEORY
SPRING TERM, 2014

JONATHAN A. PORITZ AFTER WISSAM RAJI

3. PRIMES AND THE FUNDAMENTAL THEOREM OF ARITHMETIC

Primes are the atoms out of which the more complicated, composite integers (the molecules, in this metaphor) are built. In this section we study some of their basic properties and then prove the aptly named Fundamental Theorem of Arithmetic.

First of all, we make the

Definition 3.1. We say $p \in \mathbb{N}$ is **prime** if $p > 1$ and the only natural numbers which divide p are 1 and p .

Example 3.2. Some primes are 2, 3, 5, 7, 11, 13, and 17. Notice 2 is the only even prime (clearly – any other would be a multiple of 2 and hence could not be prime), and has some unusual properties – the joke is that “2 is the oddest prime.”

The largest prime known to humans at the time of this writing is

$$2^{57,885,161} - 1$$

which was proven to be prime in January of 2013 by a distributed computer program called GIMPS [the “Great Internet Mersenne Prime Search”] running on hundreds of machines across the Internet.

In contrast, we also use the following term

Date: 24 February 2014 00:30 These notes are adapted by Jonathan Poritz from **An Introductory Course in Elementary Number Theory** by Wissam Raji, see www.saylor.org/books/. Both these notes and Raji's text are released under a Creative Commons CC BY 3.0 license, see

<https://creativecommons.org/licenses/by/3.0/>



```

\documentclass[12pt,letterpaper]{amsart}
\usepackage{times}
\usepackage{amsthm}
%\usepackage{makeidx}
\usepackage{amsmath}
\usepackage{amssymb}
\usepackage{mathrsfs}
\usepackage{amsfonts}
\usepackage{hyperref}
\usepackage{graphicx}
\usepackage{datetime}
\input jp.tex
\newtheorem{examples}[theorem]{Examples}
\newtheorem*{PHprinciple}{The Pigeonhole Principle}
\newtheorem*{WOprinciple}{The Well-Ordering Principle}
\linespread{1.3}

\title{Readings for CSU-P Math 319 Spring 2014\ \ \ \ PaR1}{Reading to Accompany CSU-P Math 319\
Number Theory\
Spring Term, 2014}

\author{Jonathan A. Poritz {\it after Wissam Raji}}

\begin{document}
\date{\thisdaymonthyear\ \ \ currenttime\ \ }
These notes are adapted by Jonathan Poritz from {\bf An Introductory
Course in Elementary Number Theory} by Wissam Raji, see
{\tt www.saylor.org/books/3}. Both these notes and Raji's text are\newline
released under a Creative Commons {\bf CC BY 3.0} license, see\newline
\hphantom{XXX}{\tt https://creativecommons.org/licenses/by/3.0/3}\vskip-9mm
\hfill\includegraphics[width=2cm,clip]{CC-BY-logo.eps}\ \ }
\maketitle

\setcounter{section}{0}
\section{Well-Ordering and Division}

\subsection{The Well-Ordering Principle and Mathematical Induction}
In this section, we present three basic tools that will often be used in proving properties of the integers. We start with a very i
important property of
integers called the well-ordering principle. We then state what is known as the pigeonhole principle, and then we proceed to presen
t an
important method called mathematical induction.

\subsubsection{\textbf{The Well-Ordering Principle}}

\begin{definition}
Given a set  $S$  of numbers (of any kind), we say that  $x$  is a
-;--- PaR1.tex      Top (1,0)      (LaTeX)
Beginning of buffer

```

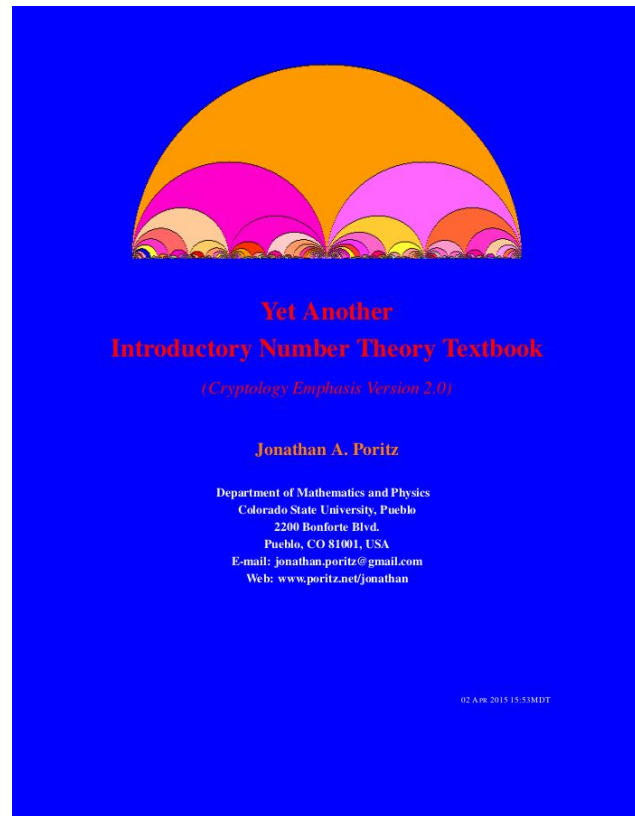
CSUP Math 319, *Number Theory*, Spring 2015

I had done this before, I had much of the material, surely I could make a good- looking book, rather than a bunch of disjointed chapters (“readings”).

While I was at it, I could include a lot of new material: the applications of number theory to cryptology that I really wanted to teach.

The goal was **Yet Another Introductory Number Theory Textbook, v2.0: Cryptology Emphasis Version.**

It still turned out to be a lot of work.



Here is a table of the frequencies of the letters in a bit of standard English (some of the plays of Shakespeare):

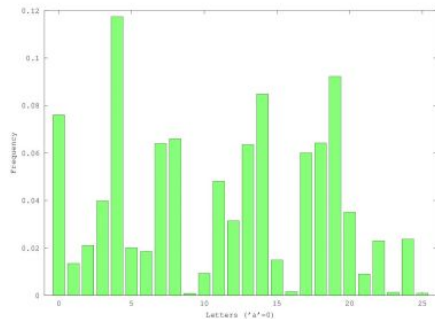


FIGURE 5.3.1. Frequency counts of letters in several Shakespeare plays

Notice that the letter 'e' is the most common, by a bit. So a first cryptanalytic approach using frequency analysis would simply be to use the Caesar decryption key which moved the most frequent letter in the ciphertext to be 'e'. With the ciphertext at the beginning of this section, that would yield the decryption:

```
e zmpczyeezmpesletdesbfpdetzy
hspescetdyzmpwctyespxtoezdfqgpc
espdwt yrdlyolcczhdzqzfeclrpzfdqzcefyp
zcezelvplcxdlrltydelplzqeczfmpwd
lyomjzaazdtyrpyoespx
```

Not so good. Apparently looking only at the most frequent letter is insufficient: the most frequent letter in the plaintext of this message was not 'e'.

Instead let us look at the entire frequency table for this ciphertext.

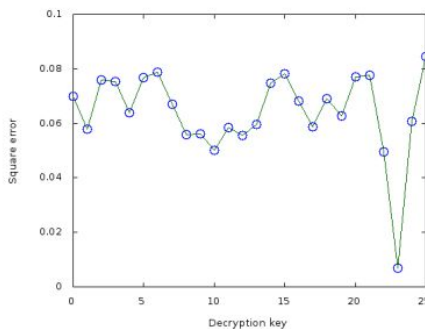


FIGURE 5.3.3. Square errors with all decryption keys for example Caesar ciphertext

The minimal square error will then come from decryption key 23 (corresponding to an original encryption key of 3; this was done by Julius himself, anachronistically). The corresponding cleartext then would have been

```
tobeornottobethatisthequestion
whethertisnoblerinthemindtosuffer
theslingsandarrowsoutrageousfortune
ortotakearmsagainstaesaoftroubles
andbyopposindgendthem
```

which looks pretty good.

Interestingly, this approach to non-gibberish detection is fairly robust, even with quite short texts which might be expected to have frequency distributions rather far away from the English standard. For example, with ciphertext

```
rkkrtbrkeffespkvytiffjjifruj
```

we have

$65537 = 10000000000000001_2$, which satisfies $\gcd(e, \phi(n)) = 1$. This number is called the **RSA exponent**.

The **RSA public [encryption] key** k_e consists of the pair (n, e) ; the set of possible such pairs is $\mathcal{K}_e$.

The **RSA private [decryption] key** k_d consists of the pair (n, d) , where

$$d = e^{-1} \pmod{\phi(n)},$$

and $\mathcal{K}_d$ is the set of such pairs.

The association of encryption to decryption keys is by $\mathcal{E} : (n, e) \mapsto (n, e^{-1} \pmod{\phi(n)})$.

The message space of this cryptosystem is $\mathcal{M} = \{m \in \mathbb{Z} \mid 0 \leq m < n\}$.

Encryption is by

$$c = e_{(n,e)}(m) = m^e \pmod{n}.$$

Decryption is

$$d_{(n,d)}(c) = c^d \pmod{n}.$$

All together, the above is called the **RSA cryptosystem**.

Graphically:

RSA cryptosystem set-up and notation:

Alice	on public network	Bob
		pick large primes p and q compute RSA modulus $n = pq$ pick RSA exponent $e \in \mathbb{N}$ with $\gcd(e, \phi(n)) = 1$ publish $k_e = (n, e)$ compute $d = e^{-1} \pmod{\phi(n)}$
download k_e	$\leftarrow$ public key $k_e \leftarrow$	
message $m \in \mathcal{M}$ compute $c = e_{(n,e)}(m)$ $= m^e \pmod{n}$ transmit c	$\mapsto$ ciphertext $c \mapsto$	receive c compute $m = d_{(n,d)}(c)$ $= c^d \pmod{n}$

The first thing we need to see is that this satisfies the basic condition to be a functioning cryptosystem:

PROPOSITION 5.4.6. *Let notation be as in the above definition of the RSA cryptosystem. Then for any message $m \in \mathcal{M}$, $d_{(n,d)}(e_{(n,e)}(m)) = m$.*

PROOF. Any $m \in \mathcal{M}$ represents a class in $\mathbb{Z}/n\mathbb{Z}$, and we will blur the distinction between the class and its representative m satisfying $0 \leq m < n$.

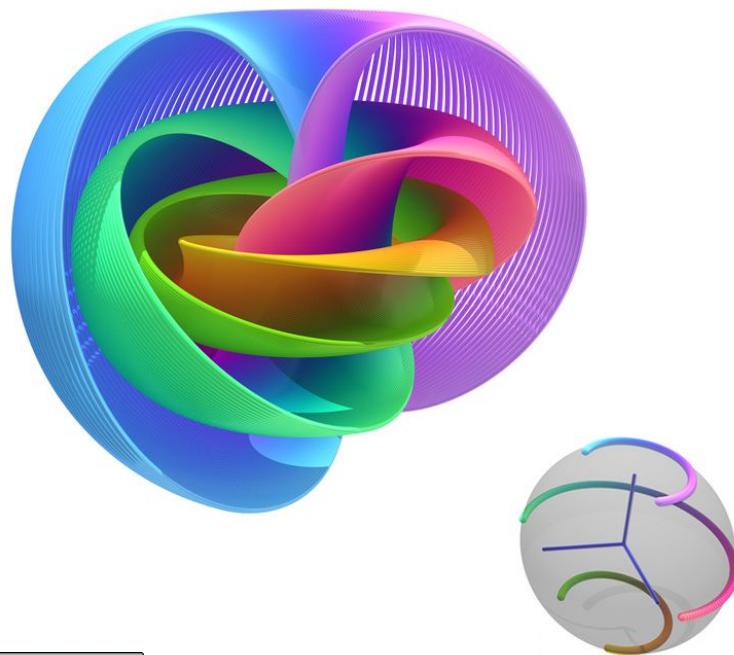
CSUP Math 411, *Intro. to Topology*, Summer 2015

Topology was always my first love, it's why I became a mathematician, it's part of me.

Surely I could teach it entirely without a book ... maybe creating notes when it would help the students and finding resources on the Internet.

To use someone else's book would be an insult to my topologist's heart.

The educational resources I used were all JITERs.



Hopf Fibration, by Niles Johnson, from [Wikimedia Commons](#), was released under a [Creative Commons Attribution-Share Alike 3.0 Unported](#) license.

CSUP Math 156, *Intro. to Statistics*, Fall 2016

This time, for the first time, I was in large part motivated by the cost of the commercial textbook I had always unquestioningly used.

I mostly assigned students to read bits out of a book from the Saylor Academy I found on the Open Textbook Library, plus lots of additional material - simplifications, alternate explanations, *etc.* - I wrote, mostly in the form of LaTeX on my website.

It was only a tiny amount more effort to use this resource plus my web pages of explanation, than it had been to use the commercial textbook.

There was a surprisingly low success rate in the online section, which might have partly been because the students had not spent the money on an expensive textbook and so had less to lose by failing...?

Reykjavik U. T-[7,8]50-CYCR, *Crypto.*, Winter 2016

Very intense experience of all JITERs and FLOSS.

Didn't see the sun in four weeks. The rain was often horizontal.

Never tried the *fermented shark*, which a student of mine told me was not made with urine as an ingredient -- it's just that the flesh of those sharks has naturally occurring urea, so it does smell like piss.

Don't get me wrong, I'd go back in a minute!

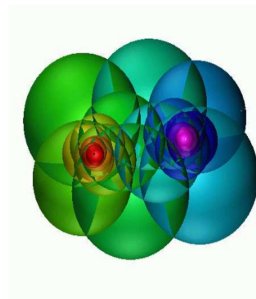
Computer science is ***so much fun*** to teach: it's all exploration, curiosity, collaboration, students going to the web for bits of code and libraries - stackoverflow.com, *etc.* It's a shame math can't be taught this way... maybe?

CSUP Math 156, *Intro. to Statistics*, Spring 2017

Much like my second go 'round with number theory, I felt that I had done this before and surely could make a good-looking book that covered what I wanted, from the perspective I wanted.

The result was **Lies, Damned Lies, or Statistics: How to Tell the Truth with Statistics**.

It still turned out to be a lot of work.



Lies, Damned Lies, or Statistics:

How to Tell the Truth with Statistics

Jonathan A. Poritz

Department of Mathematics and Physics
Colorado State University, Pueblo
2200 Bonforte Blvd.
Pueblo, CO 81001, USA
E-mail: jonathan@poritz.net
Web: poritz.net/jonathan

I've (mostly) ported **LDLoS** to *PressBooks* recently, where it will be easier to modify.

An easy thing to do with an OER statistics textbook, as I did once with **LDLoS** and could do again in the future, is to make new, topical problems every time it is used. This would prevent student cheating (e.g., with [chegg.com](https://www.chegg.com)), and promote student engagement.

I don't know that I will ever do that, because I want, the next time I teach statistics, to do a more personalized, exploratory [IBL] version, which needs either extensive JITER support, or else a very concise textbook with terse summaries of definitions, theorems, algorithms, *etc.*, plus scaffolding for student projects and exploration.



Benefits of a state-wide initiative



[Home](#) [Read Colorado Rises](#) [Best Practices](#) [Take Action](#) [Dashboard](#) [FAQ](#)



Open Educational Resources

*Powering equity
and innovation
in Colorado*



Colorado is leading the way in Open Educational Resources (OER) adoption, which has been shown to foster innovation, reduce costs and boost student success.

Lessons/Generalizations... Emily

Serving on the State OER council helped me realize:

- Impact cost of materials has on student achievement
- The importance of building relationships and teams
- A little interest and support from the state can enhance the interest of the University administration

Lessons/Generalizations ... Jonathan

It seems like two overarching themes characterize my involvement in OER:

- A. Technology issues: comfort with things like running server software, preferring markup languages to WYSIWYG interfaces, the command-line interface to point-and-click, *etc.* (*i.e.*, general geekiness)
- B. A certain monomania on the topic of autonomy, agency, and academic freedom for myself and my students. Hence FLOSS and OER.

The AAUP's 1940 *Statement of Principles on Academic Freedom and Tenure*, where academic freedom is explained and justified, says

*“Institutions of higher education are conducted **for the common good** and not to further the interest of either the individual teacher or the institution as a whole. The common good depends upon the free search for truth and its free exposition.”*

Call to action...Emily

- Help faculty find their own intrinsic motivation, which may be related to why they went into teaching in the first place
- Engage students
- Enjoy teaching
- Look for opportunities to share stories



Call to action...Jonathan

Faculty can self-educate about the tools -- we needn't accept the suppression of autonomy and agency of nonfree software (LMSes, commercial OSeS and environments, online walled gardens), we can take the time to learn how to use free software, it gives us and our students autonomy and agency.

A certain obstinacy about academic freedom, along with a bit of humane arrogance about who has the expertise, can drive us away from nonfree tools, platforms, and non-open educational resources, to a better future.

Questions/Comments/Contact Info:

Emily Ragan:

Email: eragan@msudenver.edu

Twitter: [@eragan7](https://twitter.com/eragan7)

Jonathan Poritz:

Web: <https://poritz.net/jonathan>

Email: jonathan@poritz.net

Twitter: [@poritzj](https://twitter.com/poritzj)