Math 480 - W 2014: Elementary Number Theory

- Professor: William Stein (http://wstein.org)
- Location: MWF 12:30-1:20 in Condon Hall (CDH) room 223B
- Website: https://github.com/williamstein/480-ent-2014

Textbook

- "Elementary Number Theory: Primes, Congruences, and Secrets", William Stein, pub. with Springer-Verlag
- The book free available at the course website as book.pdf. If you buy the book, tell me, so I can donate the proceeds.

Course grade

- Your 0-4 scaled grade will be entirely determined by your average score on weekly homework assignments as follows: [(98, 4), (96.5, 3.9), (95, 3.8), (93.5, 3.7), (92, 3.6), (90.5, 3.5), (89, 3.4), (87.5, 3.3), (86, 3.2), (84.5, 3.1), (83, 3.0), (81.5, 2.9), (80, 2.8), (78.5, 2.7), (77, 2.6), (75.5, 2.5), (74, 2.4), (72.5, 2.3), (71, 2.2), (69.5, 2.1), (68, 2.0), (66.5, 1.9), (65, 1.8), (63.5, 1.7), (62, 1.6), (60.5, 1.5), (59, 1.4), (57.5, 1.3), (56, 1.2), (54.5, 1.1), (53.0, 1.0), (51.5, 0.9), (50.1, 0.8), (50.0,0.7), (0, 0)]
- Your lowest 2 homework grades will be dropped. **Absolutely no late homework will receive credit.**
- Homework will be due on Wednesdays at midnight. The first assignment will be **due January 22**.
- Project: you will write a paper as part of this course.
- You will submit an updated to your paper with each homework assignment (so your paper grade is completely integrated with the homework grade).

SageMathCloud

- Create a SageMathCloud project for this course with title "480nt-Your Name", and add me as a collaborator (type "wstein@gmail.com" into the collaborators box).
- I will add to your project a directory called "homework" with the following subdirectories: due-01-22, due-01-29..., due-03-14

- You will write up your homework solutions by editing documents in each folder. At the moment it is due (midnight on the given day), I will automatically collect all the homeworks. I will then grade them and the graded version will appear next to your submission in the same directory.
- Your paper will go in a folder called "paper" in your course project.
- I may use some amount of peer grading (if you find this unacceptable, drop the class now).
- You can use git to obtain and update a complete copy of all lecture notes, etc., for this class. Do this in a terminal:

```
# Do this once the first time to get a complete copy.
cd ~; git clone https://github.com/williamstein/480-ent-2014

# Do this any time to update your copy.
cd ~/480-ent-2014; git pull
```

Office Hours

- Tuesdays in Padelford C423 1-2pm
- Just talk to me after class if possible, since I usually have nothing scheduled right after class.

Course content

- Prime numbers
- Integers modulo n
- Continued fractions
- Public key cryptography
- Elliptic curves
- LaTeX
- Sage (Python)