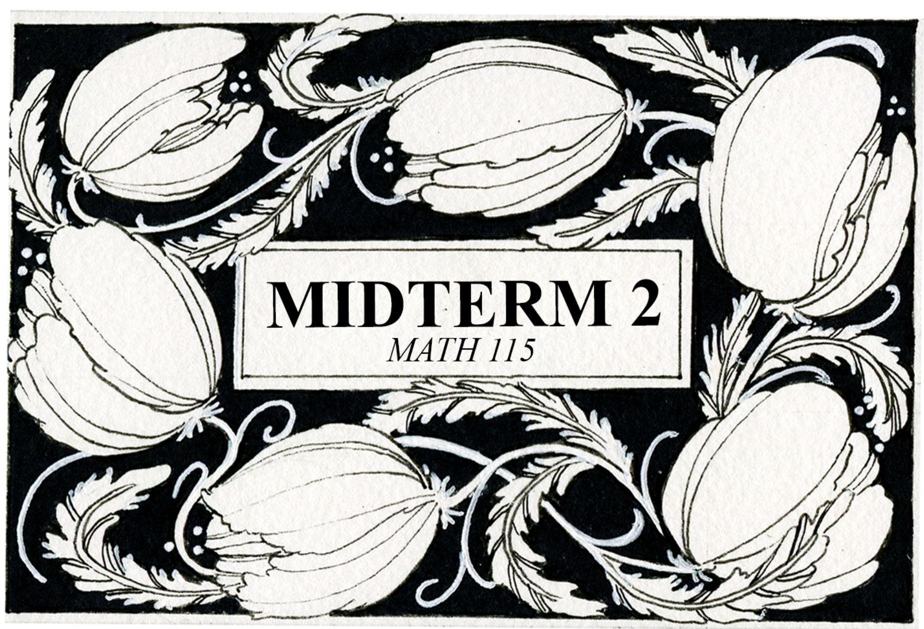
Professor Kenneth A. Ribet
March 18, 2021
8:10–9:30AM

Please do all five problems on this midterm; the problems all have the same value. You have 80 minutes to work on the exam and 15 minutes to upload your work to `Gradescope`. You may consult the textbook, all the material on `bCourses`, the class `piazza` and your own notes. In case of questions, post a private note to instructors on `piazza`. Any clarifications or corrections that need to be promulgated will be added to a pinned post on `piazza`.

Explain all your answers fully; write in complete English sentences.

Not permitted: online searches, other uses of the internet, collaboration with other people (electronic or otherwise). Please act with honesty, integrity and respect for others.



Artwork Ig: `@itchyscabs @mimithemimo`

Please remember to explain all of your answers fully.

Please remember to copy and sign the honor pledge.

1. How many primitive roots are there mod 7^7? List three of them.

2. Let p be a prime congruent to 3 mod 4 for which $2p+1$ is also prime. (For example, p could be 3 or 11.) Show that 2 is a square mod $2p+1$. Prove that $2p+1$ is a divisor of $2^p - 1$.

3. Determine the number of solutions to $x^2 \equiv 23 \pmod{691^2}$, as well as the number of solutions to $x^2 \equiv 691 \pmod{23^2}$. (The number 691 is prime.)

4. Let p be an odd prime. For $a \in \mathbf{Z}/p\mathbf{Z}$, show that the number of solutions to $y^2 = a$ in $\mathbf{Z}/p\mathbf{Z}$ is $1 + \left(\dfrac{a}{p}\right)$. If p is a prime of the form $4k+3$, prove that the number of solutions to $y^2 = x^3 - x$ with $x, y \in \mathbf{Z}/p\mathbf{Z}$ is p. (Note that $x^3 - x$ changes sign if x changes sign.)

5. Suppose that m is an odd integer such that $\left(\dfrac{a}{m}\right) = 1$ for all integers a with $\gcd(a, m) = 1$. Use the Chinese remainder theorem to show that m is a perfect square.

To finish: Please copy and sign the statement below.

> "*As a member of the UC Berkeley community, I acted with honesty, integrity, and respect for others during this exam. The work that I am uploading is my own work. I did not collaborate with or contact anyone during the exam. I did not seek or obtain solutions from* `chegg.com` *or other sites. I adhered to all instructions for this examination.*"

Please remember to explain all of your answers fully.

Please remember to copy and sign the honor pledge.