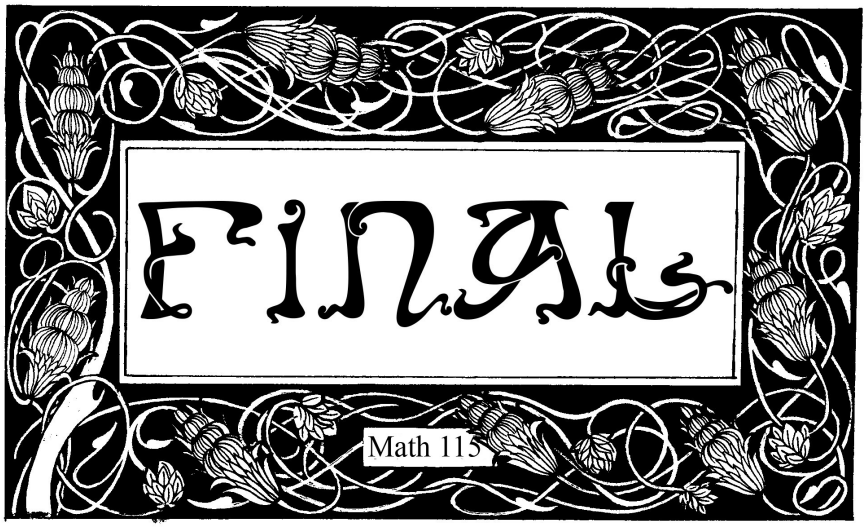
Professor Kenneth A. Ribet
May 13, 2021
7–10PM

Please do all nine problems on this final exam; the problems all have the same value. You have three hours 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. Suppose that m is a positive integer of the form $12k + 7$. Show that 3 is not a square modulo m.

2. Given Euler's theorem that all integer solutions to $y^2 = x^3 + 1$ have $x = -1, 0, 2$, use the substitutions $x = 2ab$, $y = 4b^3 + 1$ to determine the integer solutions to $a^3 - 2b^3 = 1$.

3. Consider the numbers $2^{p-1}(2^p - 1)$, where p is an odd prime number:

$$28, \quad 496, \quad 8128, \quad 2096128, \quad 33550336, \ldots.$$

Prove that they are all congruent to 1 mod 9.

4. Find the number of solutions to the congruence $x^2 - 2x - 8 \equiv 0 \pmod{63}$.

5. Determine the elements of $\mathbf{Z}[i]$ with norm $101 \cdot 109$.

6. Let p be an odd prime. Suppose that $(\mathbf{Z}/p\mathbf{Z})^*$ is written as the disjoint union of *nonempty* subsets S and T of $(\mathbf{Z}/p\mathbf{Z})^*$ and that

$$xy \in \begin{cases} S, & \text{if } x, y \in S; \\ S, & \text{if } x, y \in T; \\ T, & \text{if } x \in S \text{ and } y \in T. \end{cases}$$

a. Show that all primitive roots mod p are contained in T.

b. Show that S is the set of quadratic residues and T is the set of non-residues modulo p.

7. Let p and q be distinct odd primes, and let $m = pq$. How many elements of $(\mathbf{Z}/m\mathbf{Z})^*/\{\pm 1\}$ have square 1 (mod $\{\pm 1\}$)? Your answer might depend on p and q but should be sufficiently transparent that you can find the number of elements without hesitation if m is $59 \cdot 61$ or $61 \cdot 101$, for example.

8. Let p be a prime number. Suppose that n is an integer > 1 for which all binomial coefficients $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ are divisible by p. Show that n is a power of p.

9. Consider primitive Pythagorean triples (a, b, c) with a odd and b even. It is possible for the positive integers a, b and c to sum to a perfect square; for example, $(63, 16, 65)$ satisfies $63^2 + 16^2 = 65^2$ and $63 + 16 + 65 = 12^2$. Find a formula that generates all primitive Pythagorean triples whose entries sum to a square and use your formula to show that there are infinitely many such triples.

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.