The problems here reasonably approximate what the final will look like. Solutions will be posted on ANGEL on Thursday, April 28. These questions are fair game for discussion during the in-class review on Friday. Your notes, homework problems, and the uncollected textbook exercises are the best resource for study and practice materials.

Problem 1. Determine all integers $x$ satisfying the system of congruences

$$2x \equiv 4 \pmod{6}$$

$$3x \equiv 5 \pmod{14}.$$  

Problem 2. Observe that 2 is a square mod 17 by Gauss’ Lemma. Or, more directly, $6^2 \equiv 2 \pmod{17}$. Determine all square roots of 2 (mod 17^2).

Problem 3.  (1) Formally state the law of quadratic reciprocity.

(2) Write a paragraph explaining the law of quadratic reciprocity in a way that a freshman calculus student would understand. You may assume they know the very basics about divisibility of integers and prime numbers, but nothing else.

(3) Compute the Legendre symbol

$$\left(\frac{46}{83}\right).$$

Be sure to justify all steps in your computation.

Problem 4. Factor the integer 225 into primes in the Gaussian integers $\mathbb{Z}[i]$. Use your factorization to determine all essentially distinct ways of writing 225 as a sum of two squares.

Problem 5. Let $n$ be a positive integer, and let $x, x', y, y' \in \mathbb{Z}$ be integers.

(1) Define what $x \equiv y \pmod{n}$ means.

(2) Suppose that $x \equiv y \pmod{n}$ and $x' \equiv y' \pmod{n}$. Show that $xx' \equiv yy' \pmod{n}$.

(3) Show that if $x \in \mathbb{Z}$ is a square then $x$ is congruent to either 0 or 1 (mod 4).

Problem 6.  (1) Define what it means for two groups $G, H$ to be isomorphic.

(2) Find a product of cyclic groups of prime-power order which is isomorphic to $\mathbb{Z}_{200}^\ast$.

(3) Prove that if $a$ is an integer with $\gcd(a, 10) = 1$ then

$$a^{20} \equiv 1 \pmod{200}.$$  

Problem 7.  (1) Precisely define the Legendre symbol.

(2) State Gauss’ Lemma for computing Legendre symbols. Be sure to define any notation you use.

(3) Let $p$ be an odd prime. Use Gauss’ Lemma to prove that $-1$ is a quadratic residue mod $p$ if and only if $p \equiv 1 \pmod{4}$.

Problem 8. Prove that there are infinitely many primes of the form $4k + 1$.

Problem 9. Let $m$ be a positive integer. Show that there are only finitely many integers $n$ such that $|\mathbb{Z}_n^\ast| = m$. (Hint: think about the factorization of $n$.)

Problem 10. Efficiently determine a primitive root mod 19, and use it to compute the 3rd roots of unity mod 19.