

Math 124: Practice midterm
Number Theory Fall 2026

Logistics

The midterm will be on October 20th in class. It will begin at 9:00 A.M and end at 10:15 A.M. You should arrive at least 5 minutes before class and be ready with a pencil or pen, When you enter you will be required to give up your cell-phone, which I will collect in a basket and return to you after you have finished.

Topics to review

These topics could appear on the midterm. We reference the section numbers of *An Introduction to the Theory of Numbers*, third edition, by Niven-Zuckerman as in the course plan if you want an explicit reference.

Topic	Sections
Divisibility, gcd and lcm, Bézout's identity, Euclidean algorithm	1.1–1.2
Primes, Euclid's lemma, unique factorization, infinitude of primes	1.3
Congruence arithmetic, cancellation, residue systems, Fermat's and Euler's theorems	2.1
Linear congruences, modular inverses, Chinese remainder theorem	2.2–2.3
Euler's totient: multiplicativity, product formula, divisor-sum identity	2.4
Polynomial congruences, reduction to prime powers, lifting roots	2.5–2.6
Polynomial congruences modulo a prime and bounds on the number of roots	2.7
Orders, primitive roots, power congruences	2.9
Quadratic residues, Legendre symbols, Euler's criterion, Gauss's lemma, supplementary laws	3.1
Quadratic reciprocity and its applications	3.2
Jacobi symbols, reciprocity, and what the symbol says about solvability of quadratic equations	3.3

Trying the practice problems

Allow about 75 minutes for the six problems (100 points altogether). For exam-style practice, try them without notes, textbooks, or a calculator. Show your reasoning; you may use results from class unless asked to prove them, checking that they apply. When asked for all solutions, give every distinct residue class in $\mathbb{Z}/n\mathbb{Z}$, where n is the relevant modulus and explain why this is complete list of solutions.

1. Euclidean algorithm and linear congruences

(16 points)

(a) (8 points) Use the Euclidean algorithm to compute $\gcd(84, 33)$. Then find integers u, v such that

$$84u + 33v = \gcd(84, 33).$$

(b) Find all solutions modulo 84 to

$$33x \equiv 15 \pmod{84}.$$

Explain why there are exactly this many solutions.

2. Euler's function and Fermat's theorem

(16 points)

(a) (8 points) Compute $\varphi(180)$, and use Euler's theorem to find the least nonnegative residue of 7^{100} modulo 180.

(b) (8 points) Prove that

$$30 \mid n^5 - n$$

for every integer n . Your proof must also cover integers divisible by 2, 3, or 5.

3. Lifting roots and the Chinese remainder theorem

(16 points)

(a) (10 points) Find all solutions to

$$x^2 \equiv 6 \pmod{25}.$$

First find the roots modulo 5, then lift each root by writing $x = r + 5t$ with $0 \leq t < 5$. Show that your list is complete.

(b) (6 points) Use part (a) and the Chinese remainder theorem to find all solutions to

$$x^2 \equiv 6 \pmod{75}.$$

Give the least nonnegative representatives modulo 75.

4. Orders, primitive roots, and power congruences

(18 points)

Recall that the order of a modulo m is the least positive integer d such that $a^d \equiv 1 \pmod{m}$, when $\gcd(a, m) = 1$.

(a) (6 points) Prove that 2 is a primitive root modulo 13. Use elementary calculations with powers and congruences.

(b) (4 points) How many primitive roots are there modulo 13? What is the order of 2^4 modulo 13? Justify both answers.

(c) (8 points) Using the primitive root 2, find all solutions to

$$x^4 \equiv 3 \pmod{13}.$$

Give the least nonnegative representatives, not just powers of 2, and explain why there are no other solutions.

5. Quadratic reciprocity and Legendre symbols

(18 points)

- (a) (6 points) Use quadratic reciprocity to evaluate $\left(\frac{7}{43}\right)$. Deduce the number of solutions modulo 43 to

$$x^2 \equiv 7 \pmod{43}.$$

You do not need to find any roots explicitly.

- (b) (4 points) Evaluate $\left(\frac{-2}{73}\right)$ using the supplementary laws. Deduce the number of solutions modulo 73 to

$$x^2 \equiv -2 \pmod{73}.$$

You do not need to find any roots explicitly.

- (c) (8 points) Let p be a prime with $p \equiv 3 \pmod{4}$, and let $a \in \mathbb{Z}$ with $p \nmid a$. Prove that exactly one of a and $-a$ is a quadratic residue modulo p .

6. Jacobi symbols and solvability

(16 points)

In this problem, the symbols with composite denominators are Jacobi symbols.

(a) (8 points) Compute $\left(\frac{19}{105}\right)$ using Jacobi reciprocity, multiplicativity, and the supplementary laws, without first factoring 105. Use the result to decide whether

$$x^2 \equiv 19 \pmod{105}$$

has a solution. Explain the implication you use.

(b) (8 points) Compute $\left(\frac{2}{15}\right)$ and determine whether

$$x^2 \equiv 2 \pmod{15}$$

has a solution. Explain what this example shows about the difference between Legendre symbols and Jacobi symbols.