

Math 3527: Number Theory I

Midterm 2, Form M (Instructor: Dummit)

April 2nd, 2026

NAME (please print legibly): _____

- Show all work and justify all answers. A correct answer without sufficient work may not receive full credit!
- You may appeal to results covered at any point in the course, but please make clear what results you are using. **Box** all final numerical answers.
- In problems with multiple parts, you may use the results of previous parts in later parts, even if you did not solve the earlier parts correctly.
- You are responsible for checking that this exam has all 8 pages.
- You are allowed a 1-page note sheet. Time limit: **65 minutes**.

Pledge of Honesty

I affirm that I will not give or receive any unauthorized help on this exam, and that all work will be my own.

Signature: _____

QUESTION	VALUE	SCORE
1	12	
2	14	
3	10	
4	14	
5	12	
6	8	
7	10	
TOTAL	80	

1. (12 points) Decide whether each of the given statements is true or false, and explain (briefly) why in 1-2 sentences.

(a) There is a way to show an integer is composite without finding an explicit factorization.

(b) With current computing technology, it would be infeasible to find the prime factorization of the composite number $2^{101} - 1$, which has 31 digits.

(c) For any field F , a polynomial in $F[x]$ with no roots in F must be irreducible.

(d) For any positive integer m , there exists a primitive root in $\mathbb{Z}/m\mathbb{Z}$.

2. (14 points) Solve the following (no justification needed but it can earn partial credit):

(a) Give a Fermat factorization of $N = 93349$ given that $306^2 - N = 287$, $307^2 - N = 900$, and $308^2 - N = 1515$.

(b) Determine the multiplicative inverse of the unit $5 - 2\sqrt{6}$ in $\mathbb{Z}[\sqrt{6}]$.

(c) Find a greatest common divisor of $x^4(x - 2)^5$ and $x^3(x - 2)^2$ in $\mathbb{R}[x]$.

(d) Determine the total number of monic irreducible polynomials in $\mathbb{F}_5[x]$ of degree 3.

(e) Solve the simultaneous congruences $p \equiv 1 \pmod{x - 1}$, $p \equiv 5 \pmod{x - 3}$ in $\mathbb{Q}[x]$.

3. (10 points) Let $r = 3 + 5i$ in $\mathbb{Z}[i]$.

(a) Find a greatest common divisor of $2 + 4i$ and r in $\mathbb{Z}[i]$.

(b) Show that $2 - i$ is a unit in $\mathbb{Z}[i]$ modulo r and find its multiplicative inverse.

4. (14 points) Let $p = x^2 + 2x + 1$ in $R = \mathbb{F}_3[x]$.

(a) Find the irreducible factorization of p in R .

(b) Fill in the following portions of the addition and multiplication tables in R/pR (make sure to give as simple a residue class as possible):

+	\bar{x}	$\overline{x+1}$	$\overline{x+2}$
\bar{x}			
$\overline{x+1}$			
$\overline{x+2}$			

·	\bar{x}	$\overline{x+1}$	$\overline{x+2}$
\bar{x}			
$\overline{x+1}$			
$\overline{x+2}$			

(c) List the 6 units and 2 zero divisors in R/pR .

(d) Verify Euler's theorem for the unit $\overline{x+2}$ in R/pR .

5. (12 points) Let $R = \mathbb{Z}[\sqrt{-6}]$. Recall that in R , $N(a + b\sqrt{-6}) = a^2 + 6b^2$.

(a) Show that there are no elements of norm 2 or 5 in R .

(b) Prove that the element $2 + \sqrt{-6}$ is irreducible in R .

(c) Prove that the element $2 + \sqrt{-6}$ is not prime in R .

(d) Is R a Euclidean domain? Briefly explain why or why not.

6. (8 points) Prove that $\mathbb{F}_7[x]$ modulo $x^2 + x + 4$ is a field with exactly 49 elements.

7. (10 points) Note $7^2 \equiv 10 \pmod{13}$, $7^4 \equiv 9 \pmod{13}$, and $7^{12} \equiv 118 \pmod{169}$; you may freely use these calculations for the questions below.

(a) Show that 7 is a primitive root modulo 13^2 .

(b) Find a primitive root modulo 13^{2026} . (Briefly justify your answer.)

(c) Find the total number of primitive roots modulo 13^{2026} .

Blank page for scratch work.