Math 3527: Number Theory I

Practice Midterm 2A (Instructor: Dummit)

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 calculator and 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	15	
2	12	
3	13	
4	12	
5	8	
6	8	
7	12	
TOTAL	80	

1. (15 points) Calculate the following things (no work or justification is required):

(a) The quotient and remainder when $19 + 3i$ is divided by $4 + i$ in $\mathbb{Z}[i]$.

(b) All elements $a + b\sqrt{-2}$ with $N(a + b\sqrt{-2}) = 9$ in $\mathbb{Z}[\sqrt{-2}]$.

(c) A greatest common divisor of $3^2(2 - i)(3 + 2i)^3$ and $3(2 - i)^2$ in $\mathbb{Z}[i]$.

(d) The number of residue classes in $\mathbb{F}_7[x]$ modulo $x^3 + 5x + 2$.

(e) All of the units and zero divisors in $\mathbb{F}_3[x]$ modulo $x^2 + 2x$.

(f) The number of monic irreducible polynomials in $\mathbb{F}_2[x]$ of degree 7.

2. (12 points) Solve the following problems (justify all answers and show all work):

(a) All p with $p \equiv x \pmod{x^2}$ and $p \equiv 10 \pmod{x-2}$ in $\mathbb{R}[x]$.

(b) Determine whether there exists a primitive root modulo (each of) 34, 35, 36, and 37.

(c) Find a primitive root and the total number of primitive roots modulo $2 \cdot 3^{2026}$.

3. (13 points) Let $R = \mathbb{F}_2[x]$ and $p = x^3 + x^2 + x + 1$.

(a) List the 8 residue classes in R/pR.

(b) Express $\overline{x^2} + \overline{x^2+1}$, $\overline{x^2} \cdot \overline{x^2+1}$, and $\overline{x^2+1}^2$ as $\overline{ax^2+bx+c}$ for some $a, b, c \in \mathbb{F}_2$.

(c) Identify all of the units and zero divisors in R/pR.

(d) Verify Euler's theorem for the unit $\overline{x^2+x+1}$ in R/pR.

4. (12 points) Let $R = \mathbb{Z}[\sqrt{-7}]$.

(a) Show that the element $2 + \sqrt{-7}$ is irreducible in R.

(b) Show that the element $1 + \sqrt{-7}$ is irreducible in R. [Hint: Show that there are no elements of norm 2 or 4.]

(c) Show that the element $1 + \sqrt{-7}$ is not prime in R.

5. (8 points) Show that $\mathbb{F}_5[x]$ modulo $x^3 + x + 1$ is a field.

---

6. (8 points) Prove that 3 is a primitive root modulo 7^{2026}.

7. (12 points) Briefly justify the following statements:

(a) A zero-knowledge protocol can be used to establish knowledge of secret information without revealing useful information about it.

(b) It is possible to establish that arbitrary 500-digit integers are prime, or composite, very quickly.

(c) It is feasible to find the factorization of a 30-digit integer very quickly with modern computing technology.

(d) If a polynomial of degree 3 has no roots, then it is irreducible.

Blank page for scratch work.