Math 3527: Number Theory I

Practice Midterm 2B (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	12	
2	12	
3	12	
4	8	
5	8	
6	8	
7	8	
8	12	
TOTAL	80	

1. (12 points) For each pair of elements, use the Euclidean algorithm in the ring R to calculate a greatest common divisor d and also to find $x, y \in R$ such that $d = ax + by$.

(a) $a = x^4 + x$ and $b = x^3 + x$ in $R = \mathbb{F}_2[x]$.

(b) $a = 9 - 5i$ and $b = 3 + 2i$ in $R = \mathbb{Z}[i]$.

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

(a) The solution to $(1+i)x \equiv 3 \pmod{8+i}$ in $\mathbb{Z}[i]$.

(b) The irreducible factorizations of $x^2 - x + 4$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, and $\mathbb{F}_5[x]$.

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

(d) The number of monic irreducible polynomials in $\mathbb{F}_7[x]$ of degree 4.

3. (12 points) Show the following things:

(a) Show that the element $7 + 4\sqrt{3}$ is a unit in $\mathbb{Z}[\sqrt{3}]$ and find its multiplicative inverse.

(b) Show that the element $4 + 5i$ is irreducible and prime in $\mathbb{Z}[i]$.

(c) Show that $\mathbb{F}_5[x]$ modulo $x^4 + x + 1$ is not a field.

4. (8 points) Show that $\mathbb{Z}[i]$ modulo $3+2i$ is a field, and then verify Fermat's little theorem for the element i given that there are 13 residue classes modulo $3+2i$.

---

5. (8 points) Show that the element 4 has two inequivalent irreducible factorizations in $\mathbb{Z}[\sqrt{-3}]$. Deduce that $\mathbb{Z}[\sqrt{-3}]$ is not a Euclidean domain.

6. (8 points) Verify Euler's Theorem for the residue class of $x^2 + 1$ in $\mathbb{F}_2[x]$ modulo x^3.

---

7. (8 points) Construct, with proof, a field with exactly 125 elements.

8. (12 points) Briefly justify the following statements:

(a) It is possible to factor a large integer that is the product of two primes that are very close together, very quickly.

(b) There is no known procedure for factoring arbitrary 500-digit integers very quickly with current computing technology.

(c) There is an efficient algorithm to compute the greatest common divisor of two Gaussian integers.

(d) There exist irreducible polynomials that have no roots.

Blank page for scratch work.