Math 3527: Number Theory I

Practice Final A (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 10 pages.**
- **You are allowed a calculator and a 1-page note sheet. Time limit: 120 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	8	
3	8	
4	8	
5	15	
6	11	
7	15	
8	12	
9	8	
10	8	
11	15	
TOTAL	120	

1. (12 points) Determine the following (no justification required):

(a) The multiplicative inverse of $\overline{12}$ modulo 25.

(b) The remainder when 6^{20} is divided by 25.

(c) All n with $n \equiv 4 \pmod{19}$ and $n \equiv 3 \pmod{20}$.

(d) The value $0.1\overline{25}$ as a rational number.

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

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

2. (8 points) Recall the Fibonacci numbers F_i are defined by $F_1 = F_2 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for all $n \geq 2$. Prove that $F_1 + F_3 + F_5 + \cdots + F_{2n+1} = F_{2n+2}$ for every positive integer n.

3. (8 points) Prove that 3 has order 10 modulo 61.

4. (8 points) Construct, with proof, a field with exactly 125 elements.

5. (15 points) Determine the following (provide brief justification):

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

(b) The total number of primitive roots modulo $2 \cdot 3^{2026}$.

(c) The number of monic irreducible polynomials in $\mathbb{F}_2[x]$ of degree 10.

(d) The number of residue classes in $\mathbb{Z}[i]$ mod $7+2i$.

(e) Whether 2 is a quadratic residue modulo the primes 67 and 71.

6. (11 points) For each given a, p, and R, determine whether $\overline{a}$ is a unit or a zero divisor in the ring of residue classes R/pR. If it is a unit find $\overline{a}^{-1}$, and if it is a zero divisor find a nonzero element $\overline{b}$ with $\overline{a} \cdot \overline{b} = \overline{0}$.

(a) $a = 5567$, $p = 12445$, $R = \mathbb{Z}$.

(b) $a = 3 + 4i$, $p = 7 - 8i$, $R = \mathbb{Z}[i]$.

(c) $a = x^2 + x$, $p = x^4 + 1$, $R = \mathbb{F}_2[x]$.

7. (15 points) Calculate the following (provide brief justification):

(a) A prime factorization of 85 in $\mathbb{Z}[i]$.

(b) A way of writing $3626 = 2 \cdot 7^2 \cdot 37$ as the sum of two squares.

(c) Two Pythagorean right triangles with a side length 29.

(d) The value of the Legendre symbol $\left(\frac{141}{307}\right)$.

(e) The values of the Jacobi symbol $\left(\frac{47}{245}\right)$.

8. (12 points) Let $R = \mathbb{Z}[\sqrt{26}]$.

(a) Prove that there are no elements of norm 2 or -2 in $\mathbb{Z}[\sqrt{26}]$. [Hint: Consider $a^2 - 26b^2 = \pm 2 \bmod 13$.]

(b) Prove that $2 + \sqrt{26}$ is irreducible in $\mathbb{Z}[\sqrt{26}]$.

(c) Show that $2 + \sqrt{26}$ is not prime in $\mathbb{Z}[\sqrt{26}]$.

9. (8 points) If $p > 3$ is a prime, prove that 3 is a quadratic residue modulo p if and only if $p \equiv 1, 11 \pmod{12}$.

10. (8 points) Characterize the primes dividing an integer of the form $n^2 + 6n + 11$, for n an integer.

11. (15 points) Give brief responses justifying the following statements:

(a) There is an efficient procedure for computing the greatest common divisor of two large integers.

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

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

(d) There is a faster way to solve the congruence $x^2 \equiv 3 \pmod{11291867}$ than simply checking each possible residue class modulo 11291867 to see if it is a solution.

(e) Studying rings such as $\mathbb{Z}[i]$ and $F[x]$ can help answer number theory questions about integers.

Blank page for scratch work.