Math 3527: Number Theory I

Practice Final B (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	10	
2	8	
3	8	
4	8	
5	14	
6	10	
7	8	
8	8	
9	15	
10	8	
11	8	
12	15	
TOTAL	120	

1. (10 points) Determine the following (no justification required):

(a) The gcd and lcm of 256 and 520.

(b) All units and all zero divisors modulo 14.

(c) The value of $\varphi(5^5 7^{10})$.

(d) The solution to $5n \equiv 120 \pmod{190}$.

(e) The remainder when 2^{47} is divided by 47.

2. (8 points) Suppose $d_1 = 2$, $d_2 = 4$, and for all $n \geq 3$, $d_n = d_{n-1} + 2d_{n-2}$. Prove that $d_n = 2^n$ for every positive integer n.

3. (8 points) Show that $a^4 \equiv 0$ or $1 \pmod 5$ for every integer a. Deduce that 2024 is not the sum of three fourth powers.

4. (8 points) Prove that 3 is a primitive root modulo 7^{2026}.

5. (14 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.

(e) Solve the congruence $x^2 \cdot q(x) \equiv x + 1 \pmod{x^3 + x^2 + x + 1}$ in $\mathbb{F}_2[x]$.

6. (10 points) Determine the following (no justification required):

(a) The multiplicative inverse of $7 + 4\sqrt{3}$ in $\mathbb{Z}[\sqrt{3}]$.

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

(c) All of the unit residue classes in $\mathbb{F}_3[x]$ modulo $x^2 + 2x$.

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

(e) Which of 104, 224, 420, and 666 are the sum of two squares.

7. (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.

8. (8 points) Prove that there exists a solution to $x^2 + 6x \equiv 14 \pmod{101}$. Note 101 is prime.

9. (15 points) Calculate the following (provide brief justification):

(a) All z with $z \equiv 2 - i \pmod{3+i}$ and $z \equiv 3 \pmod{4+5i}$ in $\mathbb{Z}[i]$.

(b) A fundamental region and list of residue class representatives for $\mathbb{Z}[i]$ modulo $2 - i$.

(c) A prime factorization of $11 + 12i$ in $\mathbb{Z}[i]$.

(d) The value of the Legendre symbol $\left(\frac{103}{307}\right)$.

(e) The value of the Jacobi symbol $\left(\frac{177}{245}\right)$.

10. (8 points) If $p > 3$ is a prime, prove that -3 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 3$.

11. (8 points) Characterize the primes dividing an integer of the form $n^2 + 4n - 1$, for n an integer.

12. (15 points) Give brief responses justifying the following statements:

(a) It is believed to be difficult to decrypt an arbitrary message encoded using RSA when the key size is large.

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

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

(d) Given that 11291867 is prime, we can quickly determine whether the congruence $x^2 \equiv 3 \pmod{11291867}$ has a solution, even without a computer.

(e) Because $\left(\frac{31}{6601}\right) = -1$ but $31^{(6601-1)/2} \equiv +1 \pmod{6601}$, that means 6601 must be composite.

Blank page for scratch work.