

Math 3527: Number Theory I

Practice Midterm 1A (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 9 pages.
- You are allowed a calculator and a 1-page note sheet. Time limit: 100 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	8	
3	8	
4	12	
5	16	
6	8	
7	8	
8	8	
9	8	
10	9	
TOTAL	100	

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

(a) The gcd and lcm of $2^3 3^2 5^4 7$ and $2^4 3^3 5^4 11$.

(b) Whether $\overline{30}$ has a multiplicative inverse modulo 42.

(c) The inverse of $\overline{5}$ modulo 71.

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

(e) The value $0.\overline{125}$ as a rational number.

(f) The value of $\varphi(121)$.

2. (8 points) Prove that $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} = 2 - \frac{1}{2^n}$ for every positive integer n .

3. (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 .

4. (12 points) Find the following things (justify all answers and show all work):

(a) The gcd and lcm of 921 and 177.

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

(c) The order of 2 modulo 55.

5. (16 points) Solve the following:

- (a) Suppose p is a prime and a is an integer. If $p|a^2$, prove that $p|a$.
- (b) Prove that any two consecutive perfect squares (i.e., the integers k^2 and $(k+1)^2$) are relatively prime.
- (c) Prove that a and b are relatively prime if and only if a^2 and b^2 are relatively prime.

6. (8 points) Show that if a and b are relatively prime and divide c , then ab divides c .

7. (8 points) Show that $a^4 \equiv 0$ or $1 \pmod{5}$ for every integer a . Deduce that 2028 is not the sum of three fourth powers.

8. (8 points) Prove that 101 is the smallest prime divisor of $99! - 1$.

9. (8 points) Show that 5 is a primitive root modulo 18.

10. (9 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) It is possible to establish that arbitrary 500-digit integers are prime, or composite, very quickly.
- (c) It is believed to be difficult to decrypt an arbitrary message encoded using RSA when the key size is large.

Blank page for scratch work.