

Math 3527: Number Theory I

Practice Midterm 1B (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) All units and all zero divisors modulo 14.

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

(c) The remainder when $10!$ is divided by 11.

(d) The order of 2 modulo 13.

(e) A primitive root modulo 7.

(f) The period of the repeating decimal of $7/11$.

2. (8 points) Use the Euclidean algorithm to calculate the greatest common divisor $d = \gcd(5567, 12445)$ and also to find integers x and y such that $d = 5567x + 12445y$.

3. (8 points) Show that $a^3 - a$ is divisible by 6 for every integer a .

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

(a) The inverse of $\overline{11}$ modulo 25.

(b) The solution to $6n \equiv 10 \pmod{100}$.

(c) All n with $n \equiv 2 \pmod{9}$ and $n \equiv 7 \pmod{14}$.

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

5. (16 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 $n \geq 2$.

(a) Prove that $F_1 + F_3 + F_5 + \cdots + F_{2n+1} = F_{2n+2}$.

(b) Suppose $c_1 = c_2 = 2$, and for all $n \geq 3$, $c_n = c_{n-1}c_{n-2}$. Prove that $c_n = 2^{F_n}$ for every positive integer n .

6. (8 points) If a and b are positive integers, prove that $\gcd(a, b) = \text{lcm}(a, b)$ if and only if $a = b$.

7. (8 points) Prove that 3 has order 10 modulo 61.

8. (8 points) If u is a unit and x is a zero divisor modulo m , prove that ux is also a zero divisor modulo m .

9. (8 points) If a is a primitive root modulo a prime $p > 2$, prove that $a^{(p-1)/2} \equiv -1 \pmod{p}$. [Hint: Square $a^{(p-1)/2}$.]

10. (9 points) Briefly justify the following statements:

- (a) There is an efficient procedure for computing the greatest common divisor of two large integers.
- (b) It is feasible to find the factorization of a 40-digit integer very quickly with modern computing technology.
- (c) Breaking Rabin encryption is provably equivalent to factoring the modulus, but Rabin encryption is not suitable for modern use.

Blank page for scratch work.