

Math 3527: Number Theory I

Midterm 1 (Instructor: Dummit) – Form K

February 19th, 2026

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) Let $a = 530$ and $b = 102$.

(a) Find the greatest common divisor $\gcd(a, b)$.

(b) Find integers x and y such that $xa + yb = \gcd(a, b)$.

(c) Show that a is a zero divisor modulo b by finding an explicit nonzero element \bar{s} such that $\bar{a} \cdot \bar{s} = \bar{0}$ modulo b .

2. (12 points) Calculate the following things (no work or justification is required):

(a) Find the greatest common divisor of $2^3 \cdot 5^5 \cdot 7^3$ and $2^4 \cdot 5^5 \cdot 7^2$.

(b) Given $-483 \cdot 983 + 213 \cdot 2026 = 1$, find the multiplicative inverse of 983 modulo 2026.

(c) Given that 5 has order 1012 modulo 2026, find the order of 25 modulo 2026.

(d) Find $\varphi(3500)$.

(e) Given prime factorizations $10^4 - 1 = 3^2 \cdot 11 \cdot 101$ and $10^8 - 1 = 3^2 \cdot 11 \cdot 73 \cdot 101 \cdot 137$, find a prime p such that the repeating decimal for $1/p$ has period 8.

3. (12 points) Solve the following problems (justify all answers and show all work):

(a) Find all solutions to the congruence $6x \equiv 30 \pmod{63}$.

(b) Solve the simultaneous congruences $x \equiv 4 \pmod{12}$ and $x \equiv 1 \pmod{11}$.

(c) Find the remainder when 17^{2000} is divided by 100.

(d) Find the rational number whose decimal expansion is $0.20\overline{26} = 0.20262626\dots$.

4. (8 points) The sequence $a_0, a_1, a_2, a_3, \dots$ is defined by setting $a_0 = 5$, $a_1 = 6$, $a_2 = 8$, and for $n \geq 2$, $a_n = 3a_{n-1} - 2a_{n-2}$. Prove that $a_n = 2^n + 4$ for all integers $n \geq 0$.

5. (8 points) Suppose a, b, c are integers such that a and b both divide c . If a and b are relatively prime, prove that ab divides c .

6. (8 points) Prove that 11 is a primitive root modulo 73. You may find helpful the calculations $11^4 \equiv 41 \pmod{73}$, $11^8 \equiv 2 \pmod{73}$, $11^{16} \equiv 4 \pmod{73}$, $11^{32} \equiv 16 \pmod{73}$, $11^{64} \equiv 37 \pmod{73}$.

7. (8 points) Let $n = (60!)^{60} - 1$.

(a) Prove that n is not divisible by any prime less than 61.

(b) Prove that n is divisible by 61, and conclude that 61 is the smallest prime factor of n .

8. (12 points) Decide whether each of the given statements is true or false, and explain (briefly) why in 1-2 sentences.

(a) Even using the fastest known algorithms, the greatest common divisor of two arbitrary 500-digit numbers would take years to compute.

(b) If $a^{90} \equiv 1 \pmod{m}$, then a has order 90 modulo m .

(c) The Caesar shift is an extremely strong cryptosystem and it cannot easily be broken.

(d) Number theory and modular arithmetic can be used for cryptography.

Blank page for scratch work.