# Math 3527: Number Theory I

Midterm 1 (Instructor: Dummit) – Form J

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 $a = 520$ 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 $\overline{s}$ such that $\overline{a} \cdot \overline{s} = \overline{0}$ modulo $b$.

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

(a) Find the greatest common divisor of $2^6 \cdot 3^3 \cdot 7^2$ and $2^5 \cdot 3^3 \cdot 7^3$.

(b) Given $-797 \cdot 877 + 345 \cdot 2026 = 1$, find the multiplicative inverse of 877 modulo 2026.

(c) Given that 11 has order 46 modulo 2026, find the order of 121 modulo 2026.

(d) Find $\varphi(1500)$.

(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 $6x \equiv 36 \pmod{63}$.

(b) Solve the simultaneous congruences $x \equiv 6 \pmod{13}$ and $x \equiv 1 \pmod{12}$.

(c) Find the remainder when $13^{2000}$ is divided by 100.

(d) Find the rational number whose decimal expansion is $0.2\overline{026} = 0.2026026026\ldots$.

**4. (8 points)** The sequence $a_0, a_1, a_2, a_3, \ldots$ 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 $n = (70!)^{70} - 1$.

(a) Prove that $n$ is not divisible by any prime less than 71.

(b) Prove that $n$ is divisible by 71, and conclude that 71 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 $a^{60} \equiv 1 \pmod{m}$, then $a$ has order 60 modulo $m$.

(c) The Caesar shift is an extremely weak cryptosystem and it can easily be broken.

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

Blank page for scratch work.