MATH 4573: MIDTERM EXAM

INSTRUCTOR: TYLER GENAO

Print name: _____

OSU name.# : _____

Before you start this exam, please read the following:

- There are **five questions** on this exam, with a sixth **bonus question.**
  - For the first four, **you must show the correct work to receive credit.** Partial credit may be given for these.
  - The fifth problem is a series of True/False questions. You are not required to show your work for them, as no partial credit will be given.
  - The sixth problem is one you can do for extra credit. It is recommended that you only attempt this bonus question if you have finished the previous problems and double-checked your work.
- This is a closed notes exam. All personal electronic devices, including smart watches and cell phones, must be silenced and stored in a bag. Calculators are not permitted, and aren't necessary.
- There is a statements page and scratch paper at the back of this exam; feel free to rip them off. If you need more paper, please let me know. Scratch paper must be submitted with the exam; **however, work on scratch paper will not be graded unless you ask me to do so in your normal answer space.**

Problem:	**1**	**2**	**3**	**4**	**5**	**Bonus**	**Total**
Points:	20	15	20	20	25	10	100

I will be academically honest in all my academic work and will not tolerate academic dishonesty of others.

Signed: _____ Date: _____

Date: February 25, 2026.

Problem 1.

a) (10 points) Prove that the product of three consecutive integers is a multiple of 6.

b) (10 points) Let a and b be integers which are coprime to 3. Prove that $a^2 + b^2$ is not the square of an integer.

Problem 2. (15 points) Compute the greatest common divisor of 288 and 156, and write it as a $\mathbb{Z}$-linear combination of these two.

Problem 3. Determine whether or not each of the following systems of congruences have a solution. If they exist, then describe all solutions.

a) (10 points) The system of congruences

$$x \equiv -1 \pmod 9,$$
$$x \equiv 1 \pmod 5,$$
$$x \equiv 3 \pmod 7.$$

(Note that $9 \cdot 5 \cdot 7 = 315$, $\frac{315}{9} = 35$, $\frac{315}{5} = 63$ and $\frac{315}{7} = 45$.)

b) (10 points) The congruence $x^3 - x^2 + 2 \equiv 0 \pmod{25}$.

Problem 4.

a) (10 points) Show that for any positive integer n, if $7 \nmid n$ then

$$7 \mid (n^{6k} - 1)$$

for all integers $k \geq 0$. (*Hint:* think about this in terms of congruences.)

b) (10 points) Compute the additive order of $[55]$ in $(\mathbb{Z}/200\mathbb{Z}, +)$.

Problem 5. (5 points each) Say whether the following statements are True or False.

*****You do not need to show your work for this problem.*****

a) There exists $a \in \mathbb{Z}^+$ with $102a \equiv 1 \pmod{17}$.

b) The congruence $5x \equiv 10 \pmod{50}$ has a unique solution.

c) The multiplicative order of $[3]$ in $(\mathbb{Z}/46\mathbb{Z})^\times$ divides 22.

d) The additive group $(\mathbb{Z}/2026\mathbb{Z}, +)$ is cyclic.

e) Given $n > 1$ with prime factorization $n = \prod_{i=1}^{r} p_i^{e_i}$, one has

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i)^{e_i}.$$

Bonus Problem. Only attempt this problem if you have attempted all previous problems, and have double-checked your work. There will be less partial credit here, and it is harder than the previous questions!

(10 points) Show that for a fixed integer $n \in \mathbb{Z}^+$, the equation

$$\varphi(x) = n$$

has a finite number of solutions.

Statements

Here are some statements for reference.

1. **(Hensel's Lemma)** For a polynomial $f(x) \in \mathbb{Z}[x]$ and prime power p^e, if $f(a) \equiv 0 \pmod{p^e}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there exists an integer t unique modulo p such that $f(a+tp^e) \equiv 0 \pmod{p^{e+1}}$. One can take $t :\equiv -f'(a)^{-1} \cdot \frac{f(a)}{p^e} \pmod{p}$.
2. **(Euler's Theorem)** For integers a and m with $m > 0$, if $\gcd(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \pmod{m}$.
3. **(Linear Congruence Theorem)** For integers a, b and m with $m > 0$, the congruence $ax \equiv b \pmod{m}$ has a solution if and only if $\gcd(a, m) \mid b$. In such a case, it has exactly $\gcd(a, m)$ solutions modulo m, given by $c = \left(\frac{a}{\gcd(a,m)} \mod \frac{m}{\gcd(a,m)}\right)^{-1} \cdot \frac{b}{\gcd(a,m)} + \frac{m}{\gcd(a,m)} \cdot k$ where $k = 0, 1, 2, \ldots, \gcd(a, m) - 1$.
4. **(Chinese Remainder Theorem (CRT))** Let $m_1, m_2, \ldots, m_r > 0$ be pairwise coprime integers. Then for any integers $a_1, a_2, \ldots, a_r$, there exists a solution to the system of congruences $\{x_i \equiv a_i \pmod{m_i}\}_{i=1}^r$, and this solution is unique modulo $m := m_1 m_2 \cdots m_r$. One such solution is $x_0 := \sum_{i=1}^r \frac{m}{m_i} \cdot b_i \cdot a_i$, where each $\frac{m}{m_i} \cdot b_i \equiv 1 \pmod{m_i}$.
5. **(Wilson's Theorem)** An integer $p > 1$ is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.
6. **(Degree modulo p)** For a polynomial $f(x) = \sum_{i \geq 0} c_i x^i \in \mathbb{Z}[x]$ and a prime p, if $j \geq 0$ denotes the largest index with $c_j \not\equiv 0 \pmod{p}$, then $f(x)$ has at most j roots modulo p.
7. **(Euler's phi function formula)** For an integer $n > 1$ with prime factorization $n = \prod_{i=1}^r p_i^{e_i}$, one has $\varphi(n) = \prod_{i=1}^r p_i^{e_i - 1}(p_i - 1)$.
8. **(Lagrange's Theorem)** Let G be a finite group. Then for any element $g \in G$, its order $|g|$ divides $|G|$; thus $g^{|G|} = e$.
9. **(Binomial Theorem)** For any integer $n \geq 1$ and real numbers x and y, one has $(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$ where $\binom{n}{k} := \frac{n!}{(n-k)!k!}$.

-Scratch paper-