MATH 4573: MIDTERM

INSTRUCTOR: TYLER GENAO

Print name: _____

OSU name.# : _____

Before you start the exam, please read this:

- There are **five questions** on this exam.
  - 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.
- 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 scratch paper at the back of the midterm. If you need more, 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.**

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

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

Signed: _____ Date: _____

Problem 1. (15 points) Compute the greatest common divisor of 216 and 135, and express it in the form $216x + 135y$ for suitably chosen $x, y \in \mathbb{Z}$.

Problem 2.

a) (5 points) Show that $p \nmid (p-1)!$ for all prime $p \in \mathbb{Z}^+$.

b) (10 points) Show that $n \mid (n-1)!$ for all composite $n \in \mathbb{Z}^+$ that aren't perfect squares.

Problem 3. Characterize **all** integer solutions to the following systems of congruences. If they don't exist, then explain why.

a) (10 points) The system of congruences

$$\begin{aligned} x &\equiv -2 \pmod 4, \\ x &\equiv 2 \pmod 5, \\ x &\equiv -4 \pmod 7. \end{aligned}$$

b) (10 points) The congruence $x^3 + 4x + 1 \equiv 0 \pmod{5^2}$.

Problem 4.

a. (15 points) Determine all odd integers $n \in \mathbb{Z}^+$ for which $\phi(n) \mid n$.

b. (10 points) Assume that the unit group $G := (\mathbb{Z}/46\mathbb{Z})^\times$ is cyclic, and generated by $[5]$. Compute the multiplicative order of $[25]$ in G.

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) $x^2 + x + 1 \equiv 0 \pmod{2^{2024}}$ has a solution.

b) 5 can be written as a $\mathbb{Z}$-linear combination of 100 and 15.

c) The ring $\mathbb{Z}/29\mathbb{Z}$ is a field.

d) The prime 101 can be written as a sum of two perfect squares.

e) For all integers $a, m \in \mathbb{Z}$ with $m > 0$, one has $a^{\phi(m)} \equiv 1 \pmod{m}$.

Statements

Here are some statements for reference.

1. **(Hensel's lemma)** Let $f(x) \in \mathbb{Z}[x]$. For any $k \geq 1$, if $f(a) \equiv 0 \pmod{p^k}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there exists an integer $t \in \mathbb{Z}$, unique modulo p, for which $f(a + tp^k) \equiv 0 \pmod{p^{k+1}}$.
2. **(Linear congruence)** 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 $\gcd(a, m)$ many solutions modulo m.
3. **(Singular roots)** Let $f(x) \in \mathbb{Z}[x]$. If $a \in \mathbb{Z}$ is such that $f(a) \equiv 0 \pmod{p^k}$ and $f'(a) \equiv 0 \pmod{p}$, then there are p lifts of a to a root of $f(x)$ modulo p^{k+1}.
4. **(Chinese remainder theorem)** Let $m_1, m_2, \ldots, m_r \in \mathbb{Z}^+$ be pairwise coprime integers. Then for any integers $a_1, a_2, \ldots, a_r \in \mathbb{Z}$, the system of equations $\{x \equiv a_i \pmod{m_i}\}_{i=1}^r$ has a solution. Furthermore, if x_0 is a solution, then any other solution x_1 satisfies $x_1 \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$.
5. **(Wilson's theorem)** For any integer $p > 1$, one has that p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.
6. **(Euler's theorem)** For integers a, m with $m > 0$, if $\gcd(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$.
7. **(Dirichlet's theorem on primes in arithmetic progressions)** If $a, m \in \mathbb{Z}^+$ are coprime, then there exist infinitely many primes $p \in \mathbb{Z}^+$ such that $p \equiv a \pmod{m}$.
8. **(Degree modulo m)** For a polynomial $f(x) \in \mathbb{Z}[x]$, writing $f(x) = a_0 + a_1 x + \ldots + a_r x^r$, for an integer $m > 0$, the degree of f modulo m is the greatest integer n such that $a_n \not\equiv 0 \pmod{m}$ (if it exists).
9. **(Multiplicative inverse)** For integers a and m with $m > 0$, if $\gcd(a, m) = 1$ then there exists $b \in \mathbb{Z}$ with $ab \equiv 1 \pmod{m}$. If $\gcd(a, m) > 1$, then no such b exists.

-Scratch paper-

-Scratch paper-