Exam Sets & Numbers
(part 2: integers and modular arithmetic)

January 30, 2025, 8:30am–10:30am,
Exam Hall 4, T13-X9.

Write your name on every sheet of paper that you intend to hand in.
Please provide **complete** *arguments for each of your answers.*
You may use a simple (not programmable) calculator during the exam.
This exam consists of 3 questions. You can score up to 6 points for each question, and you obtain 2 points for free.
In this way you will score in total between 2 and 20 points.

(1) In this exercise we consider the Euclidean algorithm in a rather special case, namely for numbers of the form $10^n - 1$.
   (a) [2 points]. Assume we have integers $n > 0, m > 0, q > 0$ and $r \geq 0$ satisfying $n = qm + r$. By looking at the difference $(10^n - 1) - (10^r - 1)$, show that one can write
   $$10^n - 1 = Q \cdot (10^m - 1) + 10^r - 1,$$
   for some integer Q.
   (b) [2 points]. In a situation as in (a), show that the equality $\gcd(10^n - 1, 10^m - 1) = \gcd(10^m - 1, 10^r - 1)$ holds.
   (c) [2 points]. Use (b) to conclude that
   $$\gcd(10^n - 1, 10^m - 1) = 10^{\gcd(n,m)} - 1.$$

(2) For $k \in \mathbb{Z}_{\geq 1}$ consider the numbers $m_k := (121^k - 64^k)/57$.
   (a) [2 points]. Show that $m_k \in \mathbb{Z}$, for every $k \geq 0$.
   (b) [2 points]. Explain why no $k \geq 0$ exists such that m_k is a prime number.
   (c) [2 points]. Show that k exists such that $30012025 | m_k$. You may use that $30012025 = 5^2 \cdot 643 \cdot 1867$ (factorization into prime numbers).

(3) This is an exercise about units modulo p^3, where p is a prime number.
   (a) [2 point]. Show that the inverse of $\overline{1+p} \in (\mathbb{Z}/p^3\mathbb{Z})^\times$ equals $\overline{1-p+p^2}$.
   (b) [2 points]. Solve the system $\begin{cases} x + \bar{p}y &= \bar{a} \\ \bar{p}x + y &= \bar{b} \end{cases}$ for $x, y \in \mathbb{Z}/p^3\mathbb{Z}$ in terms of $\bar{a}, \bar{b}$.
   (c) [2 points]. Let $\bar{a} \in (\mathbb{Z}/p^3\mathbb{Z})^\times$ be arbitrary. Show that $n \in \mathbb{Z}_{\geq 0}$ exists such that $\bar{a}^{p-1} = \overline{1+np}$.

If you are only retaking the numbers part this side is all you need to complete, otherwise please turn over for part 1 on sets and do that part on a DIFFERENT piece of paper.