Problem 1. (Equivalence Relations [AM106]) Which of the following are equivalence relations? If it is an equivalence relation, describe the equivalence classes. If it is not, which property fail?

1. Domain: the positive integers. Relation: \( a \sim b \) if \( \gcd(a, b) > 1 \).
2. Domain: sets of real numbers. Relation: \( A \sim B \) if \( A \cap B = \emptyset \).
3. Domain: \( \mathbb{C} \). Relation: \( a \sim b \) if \( a = rb \) for a positive real number \( r \).

Problem 2. (Equivalence of Induction Axioms) Prove that Strong Induction implies the Well-ordering Principle.

Problem 3. (Modular Exponentiation [AM106-A])

1. Show that there is no polynomial-time algorithm that, when given \( x, y \in \mathbb{N} \), computes \( x^y \). (Hint: how many bits/digits can \( x^y \) have?)

2. Give a polynomial-time algorithm that, when given \( x, y, z \in \mathbb{N} \) with \( z > 0 \), computes \( x^y \mod z \). (Hint: use the formula \( x^y = \prod_i (x^{2^i})^{y_i} \), where \( y_i \) is the \( i \)'th bit of the binary representation of \( y \), and be careful about the length of intermediate values.)
Problem 4. (Subquadratic Integer Multiplication [AM206-A])

1. Given two $2n$-bit numbers $a, b \in \mathbb{N}$, we can write $a = a_u \cdot 2^n + a_\ell$ and $b = b_u \cdot 2^n + b_\ell$, where $a_u, a_\ell, b_u, b_\ell$ are $n$-bit integers. Then the product $a \cdot b = a_u b_u \cdot 2^{2n} + a_u b_\ell \cdot 2^n + a_\ell b_u \cdot 2^n + a_\ell b_\ell$ can be computed using 4 multiplications of $n$-bit integers and 3 additions of $2n$-bit integers. Give a different way of computing the product that involves only 3 multiplications of $(n + 1)$-bit integers and a constant number of additions of $2n$-bit integers.

2. Using the above, give an algorithm for multiplying $n$-bit integers in time $O(n^{\log_2 3}) = O(n^{1.59})$.

Problem 5. (Asymptotic Notation) True or False? Briefly justify your answers (e.g. in one sentence per part).

1. $5n + 6 = O(n)$.
2. $n^2 = O(n^3)$.
3. $n^2 = \Omega(n^3)$.
4. $n = O(\log^2 n)$.
5. $\ln n = \Theta(\log_2 n)$.
6. $5^n = 3^{O(n)}$. 