This is the part of the exam *Introduction to Mathematics* dealing with Modular Arithmetic. It consists of 3 problems, for which you can score in total 9 points. Your final grade for Modular Arithmetic will be one plus the number of points you obtain.

(1) (a) [1 point] How many elements x from the set $\mathbb{Z}/42\mathbb{Z}$ satisfy $x^2 = x$? Explain your answer.

(b) [2 points] Show that for any integer n, the only *unit* u in $\mathbb{Z}/n\mathbb{Z}$ satisfying $u^2 = u$ is $u = 1 \bmod n$.

(2) (a) [1 point] Suppose that the integers n, m are not both 0. Show that the set of common divisors of n and m is equal to the set of divisors of $\gcd(n, m)$.

(b) [2 points] Suppose that the integers a and b are not both 0, and also that the integers b and c are not both 0. Show that $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.

(3) [3 points] Show, for example using mathematical induction, that for any integer $n \geq 0$ one has

$$(1 + 4)^{2^n} \equiv 1 + 2^{n+2} \bmod 2^{n+3}.$$

(Note that the exponent on the left is 2^n, not $2n$.)