Problem 1. Let $f : R \longrightarrow S$ be a surjective homomorphism of rings. Suppose that R is unital. Prove that S is also unital and $f(1)$ is the identity element of S.

Solution: We need to show that $f(1)s = s = sf(1)$ for all $s \in S$. Since f is surjective, for any $s \in S$ there is $r \in R$ such that $s = f(r)$. Thus $f(1)s = f(1)f(r) = f(1 \cdot r) = f(r) = s$ and $sf(1) = f(r)f(1) = f(r \cdot 1) = f(r) = s$. Thus $f(1)$ is indeed the identity element of S.

Problem 2. a) Prove that $a \in \mathbb{Z}/n$ is invertible iff $\gcd(a, n) = 1$. What is the number of invertible elements of $\mathbb{Z}/n$?

b) Prove that $a \in \mathbb{Z}/n$ is a zero divisor iff $\gcd(a, n) > 1$ (and $a \neq 0$).

c) For positive integers m, n define a function $f : \mathbb{Z}/n \longrightarrow \mathbb{Z}/m$ by $f(a) \equiv a \pmod{m}$ (i.e. $f(a)$ is the remainder upon division of a by m). Prove that f is a homomorphism iff $m|n$.

Solution: a) If $a \in \mathbb{Z}/n$ is invertible then $ab = 1$ for some $b \in \mathbb{Z}/n$. On the level of integers this means that $n|(ab - 1)$. Any common divisor d of n and a is a divisor of ab and of $ab - 1$ (since $n|(ab - 1)$), so it must be 1. This proves that $\gcd(a, n) = 1$.

Conversely, suppose that $\gcd(a, n) = 1$. Then $a^{\phi(n)} = 1$ by Euler's theorem. In other words, $aa^{\phi(n)-1} = 1$, so a is invertible.

Another argument: Consider the powers $a, a^2, ...$ Since $\mathbb{Z}/n$ is finite, there are $k < l$ such that $a^k = a^l$. On the level of integers this means that $n|a^l - a^k = a^k(a^{l-k} - 1)$. Since $\gcd(a, n) = 1$, we have $\gcd(a^k, n) = 1$ and therefore $n|(a^{l-k} - 1)$. This means that $a^{l-k} = 1$ in $\mathbb{Z}/n$, so a is invertible.

By the very definition of $\phi(n)$, it equals to the number of elements in $\mathbb{Z}/n$ which are relatively prime to n hence also to the number of invertible elements in $\mathbb{Z}/n$.

b) Suppose that $a \in \mathbb{Z}/n$ is a zero divisor. Thus $a \neq 0$ and there is $b \neq 0$ such that $ab = 0$. On the level of integrs this means that $n|ab$. If we had $\gcd(a, n) = 1$ then $n|ab$ would imply that $n|b$, i.e. $b = 0$, a contradiction. Thus we must have $\gcd(a, n) > 1$ (this also follows easily from a)). Conversely, suppose that $d = \gcd(a, n) > 1$. Then $b = n/d \neq 0$ in $\mathbb{Z}/n$. Clearly $n = db|ab$, so $ab = 0$ in $\mathbb{Z}/n$. It follows that a is a zero-divisor.

Remark. Note that the argument in b) is quite simple. Now using b) we can give a proof of a) which does not use Euler's theorem. In fact, if $\gcd(a, n) = 1$ then a is not a zero divisor by b). Thus the left multiplication l_a by a is injective and therefore bijective (since $\mathbb{Z}/n$ is finite). Thus there is $b \in \mathbb{Z}/n$ such that $l_a(b) = 1$, i.e. $ab = 1$. Since $\mathbb{Z}/n$ is commutative, we see that a is invertible. If $\gcd(a, n) > 1$ then a is a zero divisor so it cannot be invertible.

c) Suppose first that $m|n$. Let $a, b \in \mathbb{Z}/n$ and let $a + b = c$, $ab = d$ (in $\mathbb{Z}/n$). Let $r = f(a), s = f(b), t = f(c), u = f(d)$. We need to prove that $r + s = t$ and $rs = u$ in $\mathbb{Z}/m$. On the level of integers this means that $r + s \equiv t \pmod{m}$ and $rs \equiv u \pmod{m}$. Note that $a \equiv r \pmod{m}$, $b \equiv s \pmod{m}$, $c \equiv t \pmod{m}$ and $d \equiv u \pmod{m}$ be the definition of f. So we have to prove that

$$a + b \equiv c \pmod{m} \quad \text{and } ab \equiv d \pmod{m} . \qquad (1)$$

Note that by the definition of addition and multiplication in $\mathbb{Z}/n$ we have

$$a + b \equiv c \pmod{n} \quad \text{and } ab \equiv d \pmod{n} . \qquad (2)$$

Since $m|n$, the congrunces (2) clearly imply congruences (1), so our proof is complete.

Suppose now that f is a homomorphism. Note that $f(1) = 1$. The key observation is the following:

In the ring $\mathbb{Z}/m$ the sum $1 + 1 + ... + 1$ (1 is added k times) equals 0 iff $m|k$ (this is immediate consequence of the definition of addition in $\mathbb{Z}/m$).

Thus $1 + 1 + .. + 1 = 0$ in $\mathbb{Z}/n$ (1 is added n times). Since f is a homomorphism, we have $0 = f(0) = f(1) + f(1) + ... + f(1) = 1 + 1 + ... + 1$ in $\mathbb{Z}/m$ (1 is added n times). By our key observation this implies that $m|n$.