1. Solve the following congruences. If there are no solutions, say so, and give some justification. (You do not need to give a complete proof.) If there are multiple solutions, be sure to find all of them.

(a) $15x + 10 = 4$ in $\mathbb{Z}_{20}$

$15x = -6 = 14$ in $\mathbb{Z}_{20}$

$15x \equiv 14 \pmod{20}$

Since $(15,20) = 5$ and $5 \nmid 14$, no solution. (Theorem 2.11)

$15x - 14 = 20k$ for some $k \in \mathbb{Z}$

$15x - 20k = 14$

Since $5 | 15$ and $5 | 20$, $5 | 15x - 20k$, but $5 \nmid 14$, so no solution.

(b) $15x + 10 = 4$ in $\mathbb{Z}_{19}$

$15x \equiv -6 \equiv 13 \pmod{19}$

$x \equiv 13 \cdot 15^{-1} \pmod{19}$

$\equiv 13 \cdot (-5) \equiv -65 \equiv 11 \pmod{19}$

$\boxed{x \equiv 11 \pmod{19}}$

$\boxed{x = 11}$

Scratch work, to find $15^{-1} \pmod{19}$:

$19 = 15 \cdot 1 + 4$	$4 = 19 - 15 \cdot 1$
$15 = 4 \cdot 3 + 3$	$3 = 15 - 4 \cdot 3$
$4 = 3 \cdot 1 + 1$	$1 = 4 - 3 \cdot 1$

$1 = 4 - 3 \cdot 1 = 4 - (15 - 4 \cdot 3) \cdot 1 = 4 \cdot 4 - 15 \cdot 1$

$= (19 - 15 \cdot 1) \cdot 4 - 15 \cdot 1 = 19 \cdot 4 - 15 \cdot 5$ ✓

$1 = 15 \cdot (-5) + 19 \cdot 4 \Rightarrow 15 \cdot (-5) \equiv 1 \pmod{19}$

So $15^{-1} \equiv -5 \equiv 14 \pmod{19}$

(c) $15x + 10 = 4$ in $\mathbb{Z}_{18}$

$15x \equiv -6 \pmod{18}$

$15x \equiv 12 \pmod{18}$

Since $(15, 18) = 3$ and $3 | 12$, there are exactly 3 distinct solutions. (Theorem 2.11)

$15x - 12 = 18k$

divide by 3

$5x - 4 = 6k$

$5x \equiv 4 \pmod 6$

$5 \cdot 5 \equiv 25 \equiv 1 \pmod 6$, so $5^{-1} \equiv 5 \pmod 6$

$x \equiv 4 \cdot 5^{-1} \pmod 6$

$\equiv 4 \cdot 5 \equiv 20 \equiv 2 \pmod 6$

$x \equiv 2 \bmod 6 \Longrightarrow \boxed{x \equiv 2 \text{ or } 8 \text{ or } 14 \pmod{18}}$

$\boxed{x = 2, x = 8, x = 14}$

2. (a) Prove that $10^n \equiv 1 \pmod 9$ for all $n \geq 0$. *(Hint: Induction)*

Base cases: $10^0 = 1 \equiv 1 \pmod 9$

$10^1 = 10 \equiv 1 \pmod 9$

Induction step: Assume true for $n-1$. So $10^{n-1} \equiv 1 \pmod 9$

$10^n \equiv 10 \cdot 10^{n-1} \equiv 1 \cdot 1 \equiv 1 \pmod 9$

True for n.

By induction, $10^n \equiv 1 \pmod 9$ for all $n \geq 0$.

(b) Let x be a positive integer, and let y be the sum of the digits of x (in base 10). Prove that $x \equiv y \pmod 9$. *(Hint: Think about how to write x in terms of its digits. Use part (a).)*

If the digits of x are $a_n a_{n-1} \cdots a_2 a_1 a_0$, then

$x = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n = \sum_{k=0}^{n} a_k 10^k$, and

$y = a_0 + a_1 + a_2 + \ldots + a_{n-1} + a_n$

By part (a), since $10^k \equiv 1 \pmod 9$ for all $k \geq 0$,

$x \equiv a_0 + a_1 \cdot 1 + a_2 \cdot 1 + \ldots + a_{n-1} \cdot 1 + a_n \cdot 1 \equiv a_0 + a_1 + a_2 + \ldots + a_{n-1} + a_n$

$\equiv y \pmod 9$

(c) Use part (b) to prove that a positive integer is divisible by 9 if and only if the sums of its digits is divisible by 9.

$9 \mid x \Leftrightarrow x \equiv 0 \pmod 9 \Leftrightarrow y \equiv 0 \pmod 9 \Leftrightarrow 9 \mid y$

By part (b)

So a positive integer (x) is divisible by 9 iff the sum of its digits (y) is divisible by 9.

3. Let R be a ring, and let $a \in R$. Let

$$S = \{ax \mid x \in R\},$$
$$T = \{xa \mid x \in R\}.$$

(a) Show that for all $r \in R$ and $s \in S$, $sr \in S$.

Let $r \in R$, $s \in S$. So $s = ax$ for some $x \in R$.

$sr = (ax)r = a(xr) \in S$ since $xr \in R$.

(b) Show that for all $r \in R$ and $t \in T$, $rt \in T$.

Let $r \in R$, $t \in T$. So $t = xa$ for some $x \in R$.

$rt = r(xa) = (rx)a \in T$ since $rx \in R$.

(c) Show that S and T are subrings of R.

It suffices to show that they are closed under subtraction and multiplication.

Let $s_1, s_2 \in S$. So $s_1 = ax_1$, $s_2 = ax_2$ for some $x_1, x_2 \in R$.

$s_1 - s_2 = ax_1 - ax_2 = a(x_1 - x_2) \in S$ because $x_1 - x_2 \in R$.

$s_1 \cdot s_2 = (ax_1) \cdot (ax_2) = a(x_1(ax_2)) \in S$ because $x_1 a x_2 \in R$.

So S is closed under subtraction and multiplication, and hence is a subring of R.

Let $t_1, t_2 \in T$. So $t_1 = x_1 a$, $t_2 = x_2 a$ for some $x_1, x_2 \in R$.

$t_1 - t_2 = x_1 a - x_2 a = (x_1 - x_2)a \in T$ because $x_1 - x_2 \in R$.

$t_1 \cdot t_2 = (x_1 a) \cdot (x_2 a) = ((x_1 a)x_2)a \in T$ because $x_1 a x_2 \in R$.

So T is closed under subtraction and multiplication, and hence is a subring of R.

4. (a) Let R be a commutative ring with identity, and let $a, b \in R$ such that ab is a unit. Show that a and b are units.

Since ab is a unit, $\exists c \in R$ such that $(ab)c = c(ab) = 1_R$.
Thus $a(bc) = 1_R$, and since R is commutative, this gives $(bc)a =$
So bc is the inverse of a, so a is a unit.

Likewise, $(ca)b = 1_R$, and by commutativity $b(ca) = 1_R$.
So ca is the inverse of b, so b is a unit.

(b) Now let R be a (not necessarily commutative) nonzero ring with identity, and assume R has no zero divisors. Let $a, b \in R$ such that ab is a unit. Show that a and b are units.

Since ab is a unit, $\exists c \in R$ s.t. $(ab)c = c(ab) = 1_R$.
Thus $a(bc) = 1_R$. We must show $(bc)a = 1_R$ also.

$$(a(bc))\cdot a = 1_R \cdot a = a$$
$$a((bc)a) = a$$
$$a((bc)a) - a = 0$$
$$a((bc)\cdot a) - a \cdot 1_R = 0$$
$$a((bc)\cdot a - 1_R) = 0$$

Since R has no zero-divisors, either $a = 0$ or $(bc)\cdot a - 1_R = 0$.
If $a = 0$, then $a(bc) = 0$, which contradicts the fact that $a(bc) = 1_R$
So $(bc)\cdot a - 1_R = 0$, so $(bc)\cdot a = 1_R$.

Thus bc is the inverse of a, so a is a unit.

Similarly, $c(ab) = 1_R \Rightarrow (ca)b = 1_R$. We must show $b(ca) = 1_R$.
$$b \cdot ((ca)b) = b \cdot 1_R = b$$
$$bcab - 1_R \cdot b = 0$$
$(bca - 1_R) \cdot b = 0$, so $b = 0$ or $bca - 1_R = 0$. But $b \neq 0$ because $(ca)b = 1_R$, so $bca - 1_R = 0$, so $b(ca) = 1_R$.

Thus ca is the inverse of b, so b is a unit.