MATH 521A: Abstract Algebra
Homework 4 Solutions

1. Use the generalized Euclidean algorithm (with $101, 999$) to find the congruence class satisfying the linear modular equation $101x \equiv 1 \pmod{999}$.

   Step 1: $999 = 9 \cdot 101 + 90$. Step 2: $101 = 1 \cdot 90 + 11$. Step 3: $90 = 8 \cdot 11 + 2$. Step 4: $11 = 5 \cdot 2 + 1$. We now back-substitute: $1 = 11 - 5 \cdot 2 = 11 - 5 \cdot (90 - 8 \cdot 11) = 41 \cdot 11 - 5 \cdot 90 = 41 \cdot (101 - 1 \cdot 90) - 5 \cdot 90 = 41 \cdot 101 - 46 \cdot 90 = 41 \cdot 101 - 46 \cdot (999 - 9 \cdot 101) = 455 \cdot 101 - 46 \cdot 999$. Taking both sides mod 999 gives us $[455] \odot [101] = [1]$.

2. Find all congruence classes satisfying the linear modular equation $24x \equiv 10 \pmod{35}$.

   We use the generalized Euclidean algorithm (or trial and error) to discover the reciprocal of 24 modulo 35, which is 19. Multiplying, we get $19 \cdot 24x \equiv 19 \cdot 10$, or $x \equiv 190 \equiv 15 \pmod{35}$. Hence we get the single equivalence class $[15]$, modulo 35.

3. Find all congruence classes satisfying the linear modular equation $25x \equiv 10 \pmod{35}$.

   We use our wonderful theorem with $a = 5$, and conclude that this linear modular equation is equivalent to $5x \equiv 2 \pmod{7}$. We now use the generalized Euclidean algorithm (or trial and error) to discover the reciprocal of 5 modulo 7, which is 3. Multiplying, we get $3 \cdot 5x \equiv 3 \cdot 2$, or $x \equiv 6 \pmod{7}$. Hence there is a single solution modulo 7, but the problem is about mod 35. There are five equivalence classes modulo 35 solving the equation, namely $[6], [13], [20], [27], [34]$.

4. Find all congruence classes satisfying the linear modular equation $25x \equiv 11 \pmod{35}$.

   We will prove that there are no solutions, by contradiction. A solution would have $35 | (25x - 11)$, which would give some $k \in \mathbb{Z}$ with $35k = 25x - 11$. Rearranging, we get $5(-7k + 5x) = 11$. This would give us $5|11$, which we know is impossible.

5. Let R be a commutative ring with identity. Prove that no element can be both a unit and a zero divisor.

   Suppose that $a \in R$ is a unit and a zero divisor. Then $a \neq 0$, and there are nonzero $b, c \in R$ with $1 = ab$ and $0 = ac$. We now have $c = c \cdot 1 = c(ab) = (ca)b = 0b = 0$. This is a contradiction, as c is nonzero.

6. Let R be a commutative ring with identity. Let $a_1, a_2 \in R$ be units, and $b_1, b_2 \in R$ be nonzero nonunits. Prove that $a_1 a_2$ is a unit, while $a_1 b_1$ and $b_1 b_2$ are nonunits.

   Since a_1, a_2 are units, there are nonzero $a_1', a_2' \in R$ with $a_1 a_1' = 1 = a_2 a_2'$. Now we have $(a_1 a_2)(a_1' a_2') = (a_1 a_1')(a_2 a_2') = 1$, so $a_1 a_2$ is a unit. Suppose now that $a_1 b_1$ were a unit. Then there would be some nonzero $c \in R$ with $a_1 b_1 c = 1$. But now $b_1(a_1 c) = 1$, so b_1 is a unit, which contradicts hypothesis. Hence $a_1 b_1$ is a nonunit. The proof for $b_1 b_2$ is similar; if it were a unit then for some $c \in R$ we would have $b_1 b_2 c = 1$, so $b_1(b_2 c) = 1$, so b_1 would be a unit. Since it's not, $b_1 b_2$ is a nonunit.

7. Let R be a commutative ring with identity. Let $a_1, a_2 \in R$ be zero divisors, and $b_1, b_2 \in R$ be nonzero and not zero divisors. Prove that a_1b_1 is a zero divisor, while b_1b_2 is not a zero divisor. Must a_1a_2 be a zero divisor?

   Since a_1 is a zero divisor, there is some a_1' with $a_1a_1' = 0$. Hence $(a_1b_1)a_1' = (a_1a_1')b_1 = 0b_1 = 0$, and also $a_1b_1 \neq 0$ (else b_1 would be a zero divisor), so a_1b_1 is a zero divisor. Note that a_1a_2 might NOT be a zero divisor, because a_1a_2 might be zero, which is not a zero divisor. Lastly, suppose that b_1b_2 were a zero divisor. Then there would be some nonzero c with $(b_1b_2)c = 0$. But then $b_1(b_2c) = 0$. Since b_2 is not a zero divisor, then b_2c is not zero, so that makes b_1 a zero divisor. This is a contradiction, so b_1b_2 is not a zero divisor.

8. Let R be a ring, with S a subring. Prove that $0_R = 0_S$, and that every zero divisor of S is also a zero divisor of R.

   We have $0_R \in S$, because that's part of the definition of subring. Also, for each $s \in S$, $0_R + s = s$, because 0_R is neutral in R. Hence 0_R is additively neutral in S; since this element is unique, in fact $0_R = 0_S$. Suppose now that $a, b \in S$ are neither 0_S, and also $ab = 0_S$. Well, since $0_R = 0_S$, we have $a, b \in R$; also neither is 0_R, and $ab = 0_R$. So if a is a zero divisor in S, then it is a zero divisor in R.

9. Let R be a ring, with S a subring. Suppose that they share a multiplicative neutral element, i.e. $1_R = 1_S$. Suppose that $a \in S$, and that a is a unit in S. Prove that a is a unit in R.

   Suppose that a is a unit in S; then neither is 0_S and there is some $b \in S$ with $ab = 1_S$. But also $a, b \in R$, neither is $0_S = 0_R$ (as proved in the previous problem), and $ab = 1_S = 1_R$. Hence a is also a unit in R.

10. Give an example of a commutative ring with identity R, with subring S, where the rings do NOT share a multiplicative neutral element. That is, with $1_R \neq 1_S$. Further, find an element $a \in S$ that is a unit in S but NOT a unit in R.

    We've already seen such an example, namely $R = \mathbb{Z}_3 \times \mathbb{Z}_3$. This has $1_R = ([1], [1])$. We now take the subring $S = \{([0], [0]), ([0], [1]), ([0], [2])\}$. This has $1_S = ([0], [1])$, which is actually a zero divisor in R. Now we can take $a = ([0], [2]) \in S$, which has $a \odot a = 1_S$, so a is a unit in S. However a is a zero divisor in R (e.g. $a \odot ([1], [0]) = 0_R$) so is certainly not a unit there.