SOLUTIONS OF HOMEWORK PROBLEMS

LAURENT VERA

CONTENTS

| Homework 1 | 1 |
| Homework 2 | 5 |
| Homework 3 | 8 |
| Homework 4 | 13 |

Note: all references to theorems use the numbering from the textbook.

Homework 1.

Problem 1.1.5. We know that \( a = bq + r \). If we multiply this equality by \( c \), we get:

\[
ac = bcq + rc
\]

Furthermore, we have \( 0 \leq r < b \). Since \( c > 0 \), multiplying this inequality by \( c \) gives us:

\[
0 \leq rc < bc
\]

So we have:

\[
ac = bcq + rc \quad \text{and} \quad 0 \leq rc < bc
\]

This means precisely that if \( ac \) is divided by \( bc \), the quotient is \( q \) and the remainder is \( rc \).

Problem 1.1.7. Let \( a \) be an integer. By the division algorithm, we know that \( a \) is of the form \( 3q, 3q + 1 \) or \( 3q + 2 \) for some integer \( q \). We treat these three cases separately.

- If \( a = 3q \), then \( a^2 = 9q^2 = 3(3q^2) \). Thus if we put \( k = 3q^2 \), we have \( a^2 = 3k \).
- If \( a = 3q + 1 \), then we have:

\[
a^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1
\]

Thus if we put \( k = 3q^2 + 2q \) we have \( a^2 = 3k + 1 \).
• If \( a = 3q + 2 \), then we have:

\[
\begin{align*}
a^2 &= (3q + 2)^2 \\
&= 9q^2 + 12q + 4 \\
&= 3(3q^2 + 4q) + 3 + 1 \\
&= 3(3q^2 + 4q + 1) + 1
\end{align*}
\]

Thus if we put \( k = 3q^2 + 4q + 1 \) we have \( a^2 = 3k + 1 \).

In conclusion, \( a^2 \) is of the form \( 3k \) or \( 3k + 1 \) for some integer \( k \).

Problem 1.2.13. (a) Let \( c \) be a common divisor of \( a \) and \( b \). Then we have \( a = cs \) and \( b = ct \) for some integers \( s \) and \( t \). If we substitute this in the equality \( a = bq + r \), we get \( cs = ctq + r \) which gives:

\[
r = cs - ctq = c(s - tq)
\]

Thus, \( c \) is also a divisor of \( r \). Since it is a divisor of \( b \) by assumption, it is a common divisor of \( b \) and \( r \). In conclusion, every common divisor of \( a \) and \( b \) is also a common divisor of \( b \) and \( r \).

(b) Let \( c \) be a common divisor of \( b \) and \( r \). Then we have \( b = cs \) and \( r = ct \) for some integers \( s \) and \( t \). If we substitute this in the equality \( a = bq + r \), we get:

\[
a = csq + ct = c(sq + t)
\]

Thus, \( c \) is also a divisor of \( a \). Since it is a divisor of \( b \) by assumption, it is a common divisor of \( a \) and \( b \). In conclusion, every common divisor of \( b \) and \( r \) is also a common divisor of \( a \) and \( b \).

(c) We know that by definition, \( (a, b) \) is a common divisor of \( a \) and \( b \). By question (a), we get that it is also a common divisor of \( b \) and \( r \). But by definition, \( (b, r) \) is the greatest common divisor of \( b \) and \( r \), so we must have \( (a, b) \leq (b, r) \).

Similarly, \( (b, r) \) is a common divisor of \( b \) and \( r \). By question (b), we get that it is also a common divisor of \( a \) and \( b \). But by definition, \( (a, b) \) is the greatest common divisor of \( a \) and \( b \), so we must have \( (b, r) \leq (a, b) \).

Thus we have \( (a, b) = (b, r) \).

Remark: this is a classic strategy to prove that two real numbers \( x_1, x_2 \) are equal. If we can prove that \( x_1 \leq x_2 \) and \( x_2 \leq x_1 \), we get \( x_1 = x_2 \).

Problem 1.2.24. Let us assume first that the equation \( ax + by = c \) has some integer solution, that we will denote by \( (x_0, y_0) \). We want to prove that \( (a, b) | c \). We know that \( (a, b) \)
is a common divisor of $a$ and $b$, so we have $a = (a, b)s$ and $b = (a, b)t$ for some integers $s$ and $t$. We can substitute this in the equation $c = ax_0 + by_0$, and we get:

\[
c = (a, b)sx_0 + (a, b)ty_0 = (a, b)(sx_0 + ty_0)
\]

Thus, we have $(a, b) | c$.

Conversely, let us assume that $(a, b) | c$, so we have $c = (a, b)t$ for some integer $t$. We want to show that the equation $ax + by = c$ has some integer solution. By theorem 1.2, we can find some integers $u$ and $v$ such that $(a, b) = au + bv$. If we multiply this equality by $t$, we get:

\[
(a, b)t = aut + bvt
\]

Since $c = (a, b)t$, this gives:

\[
c = aut + bvt
\]

In other words, we have found an integer solution to the equation $ax + by = c$, namely $x = ut$ and $y = vt$.

In conclusion, we have proved that the equation $ax + by = c$ has some integer solution if and only if $(a, b) | c$.

**Problem 1.2.31.** (a) $[6, 10] = 30$

$[4, 5, 6, 10] = 60$

$[20, 42] = 420$

$[2, 3, 14, 36, 42] = 252$

(b) Let $t$ be an integer multiple of each $a_i$. Denote $[a_1, \ldots, a_k]$ by $m$. We want to prove that $m | t$, which we do by proving that the remainder of the division of $t$ by $m$ is zero. The division algorithm gives:

\[
t = mq + r \quad \text{and} \quad 0 \leq r < m
\]

So we have $r = t - mq$. Since each $a_i$ divides both $t$ and $m$, it divides also $r$. But $m$ is the smallest positive integer with this property, and we have $r < m$. Necessarily, $r = 0$. Thus $m | t$.

**Problem 1.2.34.** (a) Since $(a, b)$ is a divisor of $a$ and $b$, there are integers $s$ and $t$ such that $a = (a, b)s$ and $b = (a, b)t$. Hence, $a + b = (a, b)(s + t)$, so $(a, b)$ divides $a + b$. Similarly, $a - b = (a, b)(s - t)$ so $(a, b)$ divides $a - b$. By the corollary 1.3, we get $(a, b) | (a + b, a - b)$.

(b) We use the following fact: if $m, n$ are two positive integers such that $n | m$ and $m | n$ then $m = n$. We already know $(a, b) | (a + b, a - b)$ from question (a), so it suffices to prove that $(a + b, a - b) | (a, b)$.

First, we know that $(a + b, a - b)$ divides $a + b$ and $a - b$. So it divides $(a + b) + (a - b) = 2a$, i.e. there is an integer $k$ such that $k(a + b, a - b) = 2a$. But since $a$ is odd and $b$ is even,
$a+b$ is odd, and thus $(a+b,a-b)$ is odd too. Furthermore, $k(a+b,a-b)$ is even (because it is equal to $2a$). This forces $k$ to be even (because the product of two odd integers is odd). So we can write $k = 2k'$ for some integer $k'$. Then we get $2k'(a+b,a-b) = 2a$, which gives $k'(a+b,a-b) = a$. So $(a+b,a-b)|a$.

We can prove entirely similarly that $(a+b,a-b)|b$. By corollary 1.3, we deduce that $(a+b,a-b) = (a,b)$.

(c) We know from question (a) that $k(a,b) = (a+b,a-b)$ for some integer $k$. Since $a$ is odd, $(a,b)$ is odd. But $b$ is also odd, so $a+b$ and $a-b$ are both even. Thus, $(a+b,a-b)$ is even. Thus $k(a,b)$ is even, so $k$ has to be even and we have $k = 2k'$ for some integer $k'$.

From the equality $k(a,b) = (a+b,a-b)$ we get $2k'(a,b) = (a+b,a-b)$. So $2(a,b) = (a+b,a-b)$.

Conversely, we have seen in question (b) that $(a+b,a-b)|2a$. Since $(a+b,a-b)$ is even, we have $(a+b,a-b) = 2q$ for some integer $q$. And from $2q|2a$ we get $q|a$. Similarly, we have $q|b$. Thus $q|(a,b)$. By multiplying by 2 we get $2q|2(a,b)$, i.e. $(a+b,a-b)|2(a,b)$.

In conclusion, $(a+b,a-b) = 2(a,b)$.

**Problem 3.** (a) Let $d$ be a common divisor of $a$ and $b$. We have $a = dk$ and $b = dl$ for some integers $k$ and $l$. If we substitute this in the equation $1 = as + bt$ we get:

$$1 = dks + dlt$$

Thus $d|1$. So the only common divisors of $a$ and $b$ are 1 and $-1$. This implies that $(a,b) = 1$, i.e. $a$ and $b$ are relatively prime.

(b) Since $(a,c) = 1$, we know from theorem 1.2 that we can write $1 = as + ct$ for some integers $s$ and $t$. Similarly, since $(b,c) = 1$ we have $1 = bs' + ct'$ for some integers $s'$ and $t'$. If we multiply these two equalities we get:

$$1 = (as + ct)(bs' + ct')$$

$$= asbs' + asct' + ctbs' + c^2tt'$$

$$= ab(ss') + c(ast' + tbs' + ctt')$$

$$= abs'' + ct''$$

where we put $s'' = ss'$ and $t'' = ast' + tbs' + ctt'$. By question (a), this implies that $ab$ and $c$ are relatively prime.

**Remark:** we could have done question (a) by using the result we proved in problem 1.2.24 (we basically just did the same proof in the particular case of relatively prime integers).
Homework 2.

Problem 1.3.9. Assume $p$ is prime, and let $r, s$ be integers such that $p = rs$. Then $p|rs$ and since $p$ is prime we have $p|r$ or $p|s$ by theorem 1.5. But since $r|p$ and $s|p$, this implies that $r = \pm p$ or $s = \pm p$. Since $p = rs$, we get $s = \pm 1$ or $r = \pm 1$.

Conversely, assume that whenever $p = rs$ for some integers $r, s$, then $r = \pm 1$ or $s = \pm 1$. Let us prove that $p$ is prime. Let $d$ be a divisor of $p$. Then $p = dk$ for some integer $k$. Using the assumption, we get $d = \pm 1$ or $k = \pm 1$. And in the case where $k = \pm 1$, the equality $p = dk$ gives $d = \pm p$. So we have either $d = \pm 1$ or $d = \pm p$. Hence the only divisors of $p$ are $\pm 1$ and $\pm p$, which means that $p$ is prime.

Problem 1.3.25. For $1 \leq k < p$, we have:

\[
\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!}
\]

which gives:

\[
pu = \binom{p}{k}k!
\]

where $u = (p-1)\ldots(p-k+1)$. So we have $p|(\binom{p}{k})k!$. Since $p$ is prime, we have either $p|(\binom{p}{k})$ or $p|k!$ by theorem 1.5. But since $p$ is prime, if we had $p|k! = k(k-1)\ldots2 \cdot 1$, we would have $p|j$ for some $j \in \{1, \ldots, k\}$ by theorem 1.5. This is impossible since $k < p$. Thus we have $p|(\binom{p}{k})$.

Problem 1.3.27. Since $p$ is a prime larger than 3, 3 does not divide $p$. So the remainder of the division of $p$ by 3 is either 1 or 2.

- **Case 1:** the remainder is 1. Then $p = 3k + 1$ for some integer $k$. Then we have:

\[
p^2 + 2 = (3k + 1)^2 + 2 = 9k^2 + 6k + 3 = 3(3k^2 + 2k + 1)
\]

Hence $3|p^2 + 2$. Since $p^2 + 2 > 3$, this implies that $p^2 + 2$ is composite.

- **Case 2:** the remainder is 2. Then $p = 3k + 2$ for some integer $k$. Then we have:

\[
p^2 + 2 = (3k + 2)^2 + 2 = 9k^2 + 12k + 6 = 3(3k^2 + 2k + 2)
\]

Hence $3|p^2 + 2$. Since $p^2 + 2 > 3$, this implies that $p^2 + 2$ is composite.

So $p^2 + 2$ is composite.
Problem 2.1.2. (a) By theorem 2.2, if \( k \equiv 1 \pmod{4} \) then \( 6^k \equiv 6 \equiv 2 \pmod{4} \), and \( 6k + 5 \equiv 2 + 5 \equiv 7 \equiv 3 \pmod{4} \). Thus \( 6k + 5 \) is congruent to 3 modulo 4.

(b) By theorem 2.2, if \( r \equiv 3 \pmod{10} \) and \( s \equiv -7 \pmod{10} \) then we have:
\[
2r + 3s \equiv 2 \cdot 3 - 3 \cdot 7
\equiv -15
\equiv 5
\]
all these congruences being modulo 10. Thus \( 2r + 3s \) is congruent to 5 modulo 10.

Problem 2.1.10. Let \( x_0, \ldots, x_n \) be the digits of \( a \). For instance, if \( a = 2235 \), we have \( n = 3 \), \( x_0 = 5 \), \( x_1 = 3 \), \( x_2 = 2 \) and \( x_3 = 2 \). Then we have:
\[
a = \sum_{j=0}^{n} x_j 10^j
\]

Note that:
\[
\sum_{j=1}^{n} x_j 10^j = 10 \left( \sum_{j=1}^{n} x_j 10^{j-1} \right)
\]
Thus we have:
\[
\sum_{j=1}^{n} x_j 10^j \equiv 0 \pmod{10}
\]
Adding \( x_0 \) to this congruence relation gives:
\[
a = \sum_{j=0}^{n} x_j 10^j \equiv x_0 \pmod{10}
\]
So \( a \) is congruent to its last digit \( x_0 \) modulo 10.

Problem 2.1.14. (a) This result is false in general. For instance, take \( n = 6 \). We have \( 2 \cdot 3 \equiv 0 \pmod{6} \), but neither 2 nor 3 are congruent to 0 modulo 6.

(b) However, if \( n \) is prime, the result holds. Indeed, if \( a, b \) are integers such that \( ab \equiv 0 \pmod{n} \), then \( n \mid ab \). Since \( n \) is prime, we have either \( n \mid a \) or \( n \mid b \), i.e. \( a \equiv 0 \pmod{n} \) or \( b \equiv 0 \pmod{n} \).

Problem 2.1.21. (a) This will be a consequence of the following general fact: if \( a \equiv b \pmod{c} \) for some integers \( a, b, c \) with \( c > 0 \), then \( a^n \equiv b^n \pmod{c} \) for every positive integer \( n \).

Proof of this fact: either by induction on \( n \) using theorem 2.2 (try it!), or by noticing that we have:
\[
a^n - b^n = (a - b) \sum_{j=0}^{n-1} a^j b^{n-1-j}
\]
(this is a classical formula that can be proved easily by induction on \( n \)). In particular \((a - b)\mid (a^n - b^n)\). Since \( c\mid (a - b) \), it follows that \( c\mid (a^n - b^n) \), which means precisely that \( a^n \equiv b^n \pmod{c} \).

Now since we have \( 10 \equiv 1 \pmod{9} \), using this fact gives us \( 10^n \equiv 1^n = 1 \pmod{9} \) for every positive integer \( n \).

\[(b) \text{ Let } a \text{ be a positive integer and } x_0, \ldots, x_n \text{ its digits. We have:} \]

\[a = \sum_{j=0}^{n} x_j 10^j\]

By (a) we have \( 10^j \equiv 1 \pmod{9} \) for every positive \( j \). Thus \( x_j 10^j \equiv x_j \pmod{9} \) for every \( j \in \{0, \ldots, n\} \). Adding all of these congruence relations for \( j \) from 0 to \( n \) gives:

\[a = \sum_{j=0}^{n} x_j 10^j \equiv \sum_{j=0}^{n} x_j \pmod{9}\]

So \( a \) is congruent to the sum of its digits modulo 9.

Remark: the same result holds with 3 instead of 9, since \( 10 \equiv 1 \pmod{3} \).

Problem 3. Let \( x \) be an integer such that \( x^2 \equiv 35 \pmod{100} \). Then \( x^2 = 100k + 35 \) for some integer \( k \). This can be written \( x^2 = 10(10k + 3) + 5 \), and thus \( x^2 \equiv 5 \pmod{10} \). The following table gives the "graph" of the function \( u \mapsto u^2 \) modulo 10.

<table>
<thead>
<tr>
<th>( u \pmod{10} )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>( u^2 \pmod{10} )</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>6</td>
<td>5</td>
<td>6</td>
<td>9</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Since \( x^2 \equiv 5 \pmod{10} \), this table gives \( x \equiv 5 \pmod{10} \). So \( x = 10q + 5 \) for some integer \( q \). It follows that:

\[x^2 = (10q + 5)^2 = 100q^2 + 100q + 25 = 100(q^2 + q) + 25\]

So \( x^2 \equiv 25 \pmod{100} \). This is a contradiction. Hence the equation \( x^2 \equiv 35 \pmod{100} \) has no solutions.
Homework 3.

Problem 1. The following table gives all the possibilities for $a^2$ modulo 8:

<table>
<thead>
<tr>
<th>$a \pmod{8}$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a^2 \pmod{8}$</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

So for any integer $a$, we have $a^2$ congruent to 0, 1 or 4 modulo 8.

We want to prove that there exists no integers $x, y, z$ such that $x^2 + y^2 + z^2 = 999$. On the one hand, we have $999 \equiv 7 \pmod{8}$. On the other hand, the 10 possibilities for $x^2 + y^2 + z^2$ modulo 8 depending on the classes of $x^2, y^2$ and $z^2$ are the following:

- If the three are congruent to 0, their sum is congruent to 0.
- If two are congruent to 0 and the third is congruent to 1, their sum is congruent to 1.
- If two are congruent to 0 and the third is congruent to 4, their sum is congruent to 4.
- If one is congruent to 0 and two are congruent to 1, their sum is congruent to 2.
- If one is congruent to 0 and two are congruent to 4, their sum is congruent to 0.
- If one is congruent to 0, one is congruent to 1 and one is congruent to 4, their sum is congruent to 5.
- If two are congruent to 0, one is congruent to 1 and one is congruent to 4, their sum is congruent to 6.
- If two are congruent to 1 and one is congruent to 4, their sum is congruent to 1.
- If the three are congruent to 1, their sum is congruent to 3.
- If the three are congruent to 4, their sum is congruent to 4.

So for any integers $x, y, z$, $x^2 + y^2 + z^2$ is not congruent to 7 modulo 8. It follows that the equation $x^2 + y^2 + z^2 = 999$ has no integer solutions.

Problem 2.2.3. We use the table from the previous exercise: the solutions to $x^2 = [1]$ in $\mathbb{Z}_8$ are $[1], [3], [5]$ and $[7]$.

Problem 2.2.5. Let us look at all the possibilities for $a^2 + 3a + 2$ modulo 6:

<table>
<thead>
<tr>
<th>$a \pmod{6}$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a^2 + 3a + 2 \pmod{6}$</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

So the solutions to $x^2 + [3]x + [2] = [0]$ in $\mathbb{Z}_6$ are $[1], [2], [4], [5]$.

Problem 2.2.9. (a) For instance, $[3]$ will work. Indeed, we have:

- $3^0 \equiv 1 \pmod{7}$
- $3^1 \equiv 3 \pmod{7}$
- $3^2 \equiv 2 \pmod{7}$
- $3^3 \equiv 6 \pmod{7}$
Thus we have obtained all the nonzero congruence classes modulo 7 by taking powers of 
\[ 3 \].

(b) In \( \mathbb{Z}_5 \), \( [2] \) will work. Indeed, we have:
- \( 2^0 \equiv 1 \) (mod 5)
- \( 2^1 \equiv 2 \) (mod 5)
- \( 2^2 \equiv 4 \) (mod 5)
- \( 2^3 \equiv 3 \) (mod 5)

Thus we have obtained all the nonzero congruence classes modulo 5 by taking powers of 
\( [2] \).

(c) We cannot find such a class in \( \mathbb{Z}_6 \). One could argue by computing the powers of each 
nonzero element of \( \mathbb{Z}_6 \) and see that none of them gives all the nonzero congruence classes.

A more conceptual reason for this is that if \( n \) is a positive integer and we have a class 
\( x \in \mathbb{Z}_n \) such that every nonzero element of \( \mathbb{Z}_n \) is a power of \( x \), then \( n \) is prime. Proof 
of this fact: since every nonzero element of \( \mathbb{Z}_n \) is a power of \( x \) by assumption, there is a 
positive integer \( r \) such that \( x^r = 1 \). It follows that \( x \) is a unit in \( \mathbb{Z}_n \). But the powers of a 
unit are also units. So every nonzero element of \( \mathbb{Z}_n \) is a unit. By theorem 2.8, \( n \) is prime.

Problem 2.3.1. Using theorem 2.10, we get that:
(a) The units in \( \mathbb{Z}_7 \) are all the nonzero classes since 7 is prime. So \( [1], [2], [3], [4], [5], [6] \) 
are the units in \( \mathbb{Z}_7 \).
(b) The units in \( \mathbb{Z}_8 \) are \( [1], [3], [5], [7] \).
(c) The units in \( \mathbb{Z}_9 \) are \( [1], [2], [4], [5], [7], [8] \).
(b) The units in \( \mathbb{Z}_{10} \) are \( [1], [3], [7], [9] \).

Problem 2.3.2. (a) There are no zero divisors in \( \mathbb{Z}_7 \) since all nonzero elements are units.
(b) The zero divisors in \( \mathbb{Z}_8 \) are \( [2], [4], [6] \).
(c) The zero divisors in \( \mathbb{Z}_9 \) are \( [3], [6] \).
(b) The zero divisors in \( \mathbb{Z}_{10} \) are \( [2], [4], [5], [6], [8] \).

Problem 2.3.3. The observations you make in the previous 2 problems should lead you to 
the following conjecture: every non zero element in \( \mathbb{Z}_n \) is either a unit or a zero divisor.

Proof of this conjecture: let \( x \) be a non zero element of \( \mathbb{Z}_n \). Then there is a (non unique) 
integer \( a \) such that \( x = [a] \). There are two possibilities: either \( a \) and \( n \) are relatively prime, 
or they are not.
- if \( (a, n) = 1 \), then we know that \( x \) is a unit from theorem 2.10.
• if \( a \) and \( n \) are not relatively prime, they have a common divisor \( d \) with \( d > 1 \). So we have integers \( u, v \) such that \( n = du \) and \( a = dv \). Since \( d \) is a divisor of \( n \), we have \( d \leq n \). We cannot have \( d = n \), otherwise \( a \) would be a multiple of \( n \) and we would have \( x = 0 \). So we have \( 1 < d < n \). Thus we have \( 1 < u < n \). In particular, \([u]\) is a nonzero element of \( \mathbb{Z}_n \). Now observe that:

\[
\begin{align*}
x[u] &= [a][u] \\
&= [au] \\
&= [dvu] \\
&= [nv] \\
&= 0
\end{align*}
\]

Thus \( x \) is a zero divisor in \( \mathbb{Z}_n \).

So the conjecture is proved.

Problem 2.3.5. First, we claim that \( ab \neq 0 \). Indeed, since \( a \) is a unit, the equation \( ax = 0 \) has \( x = 0 \) as a unique solution. But \( b \neq 0 \) since \( b \) is a zero divisor. Thus \( ab \neq 0 \). Then, since \( b \) is a zero divisor, there is a nonzero element \( c \) such that \( bc = 0 \). Hence we have \((ab)c = a(bc) = 0\). So \( ab \) is a zero divisor.

Problem 3.1.1. (a) The set of odd integers and 0 is not stable under addition since the sum of two odd integers is even.

(b) For any positive integer \( a \), there is no solution to the equation \( a + x = 0 \) in the set of non negative integer.

Problem 3.1.9. (b) First, it is clear that \( R^* \) is not empty since it contains the element \((0_R, 0_R)\). Let \( x \) and \( y \) be elements of \( R^* \), we check that \( x - y \in R \) and \( xy \in R \). There are elements \( r, s \) of \( R \) such that \( x = (r, r) \) and \( y = (s, s) \) by definition of \( R^* \). So we have:

\[
x - y = (r, r) - (s, s) = (r - s, r - s) \in R^*
\]

Furthermore:

\[
xy = (r, r)(s, s) = (rs, rs) \in R^*
\]

Hence, \( R^* \) is a subring of \( R \times R \).

Problem 3.1.17. We write \( a \ast b \) for this new multiplication. Clearly, the properties relative to the addition are still satisfied since we endowed \( \mathbb{Z} \) with the ordinary addition. We just have to check closure for multiplication, associativity, distributivity and commutativity.

- Closure for multiplication is obvious since for all \( a, b \in \mathbb{Z}, a \ast b = 0 \in \mathbb{Z} \).
- Let \( a, b, c \in \mathbb{Z} \), then we have: \((a \ast b) \ast c = 0 = a \ast (b \ast c)\). So \( \ast \) is associative.
- Let \( a, b, c \in \mathbb{Z} \), then we have: \( a \ast (b + c) = 0 = a \ast b + a \ast c \). So \( \ast \) is distributive with respect to the addition.
• Let \( a, b \in \mathbb{Z} \). Then we have \( a \star b = 0 = b \star a \). So \( \star \) is commutative.

Thus \( \mathbb{Z} \) endowed with the usual addition and the multiplication \( \star \) is a commutative ring (it does not have a unit though).

**Problem 3.1.18.** Write \( a \ast b \) for the multiplication here. The distributivity axiom is going to fail for this new multiplication. Indeed, if \( a, b, c \) are integers, we have \( a \ast (b + c) = 1 \), but \( a \ast b + a \ast c = 2 \). So we do not get a ring.

**Problem 3.1.35.** (a) This is false. Actually, if \( R \) and \( S \) are integral domains, then \( R \times S \) is not a domain. Indeed, consider \( a = (1_R, 0_S) \) and \( b = (0_R, 1_S) \). Then we have \( ab = 0_{(R \times S)} \), but neither \( a \) nor \( b \) are zero since in a unital nonzero ring the unit and the zero element are distinct.

(b) False for the same reason as above, since a field is in particular an integral domain.

**Problem 5.** (a) First, it is clear that \( R \) is non empty (we have \( 0 \in R \)). Let \( x, y \in R \), let us show that \( x - y \in R \) and \( xy \in R \). By definition of \( R \), there are integers \( a, b, c, d \) such that \( x = a + b\sqrt{2} \) and \( y = c + d\sqrt{2} \). Then we have:

\[
x - y = a + b\sqrt{2} - (c + d\sqrt{2})
= (a - b) + (c - d)\sqrt{2}
\]

Since \( a - b \in \mathbb{Z} \) and \( c - d \in \mathbb{Z} \), we have \( x - y \in R \).

For the multiplication, we have:

\[
xy = (a + b\sqrt{2})(c + d\sqrt{2})
= ac + ad\sqrt{2} + bc\sqrt{2} + 2bd
= (ac + 2bd) + (ad + bc)\sqrt{2}
\]

Since \( ac + 2bd \in \mathbb{Z} \) and \( ad + bc \in \mathbb{Z} \), we have \( xy \in R \).

So \( R \) is a subring of \( \mathbb{R} \).

Let us check that it is furthermore a domain. It has a unit \( 1 = 1 + 0\sqrt{2} \), and if we have \( ab = 0 \) with \( a, b \in R \), then since \( \mathbb{R} \) is a domain we have \( a = 0 \) or \( b = 0 \). So \( R \) is a domain.

**Remark:** The argument just given shows more generally that a unital subring of a domain is itself a domain.
(b) We claim that $S$ is not closed under multiplication. Indeed, we have $\frac{1}{2} \in S$, but $\frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2}$ is not an element of $S$. If it were, there would be integers $a, b$ such that:

$$\frac{1}{4} = \frac{1}{2} (a + b \sqrt{2})$$

We can rearrange this to:

$$b \sqrt{2} = \frac{1}{2} - a$$

Since $\sqrt{2}$ is not rational, we have $b = 0$. Thus we get $a = \frac{1}{2}$ which is a contradiction since $a$ is an integer. So we have proved that $S$ is not closed under multiplication. In particular, it is not a subring of $\mathbb{R}$. 
**Homework 4.**

*Problem 3.2.3(b).* If \(a\) is an integer, we just write \(a\) for the class of \(a\) in \(\mathbb{Z}_{12}\). We test all the elements of \(\mathbb{Z}_{12}\) to see if they are idempotents or not.

- \(0^2 = 0\) so 0 is an idempotent.
- \(1^2 = 1\) so 1 is an idempotent.
- \(2^2 = 4 \neq 2\) so 2 is not an idempotent.
- \(3^2 = 9 \neq 3\) so 3 is not an idempotent.
- \(4^2 = 16 = 4\) so 4 is an idempotent.
- \(5^2 = 25 = 1 \neq 5\) so 5 is not an idempotent.
- \(6^2 = 36 = 0 \neq 6\) so 6 is not an idempotent.
- \(7^2 = (-5)^2 = 1 \neq 7\) so 7 is not an idempotent.
- \(8^2 = (-4)^2 = 4 \neq 8\) so 8 is not an idempotent.
- \(9^2 = (-3)^2 = 9\) so 9 is an idempotent.
- \(10^2 = (-2)^2 = 4 \neq 10\) so 10 is not an idempotent.
- \(11^2 = (-1)^2 = 1 \neq 11\) so 11 is not an idempotent.

Hence the idempotents of \(\mathbb{Z}_{12}\) are 0, 1, 4 and 9.

*Problem 3.2.8.* Let us prove that \(T\) satisfies the conditions of theorem 3.6. Clearly, \(T\) is not empty since \(0 = 0b \in T\). Furthermore, if \(x, y \in T\), let us show that \(x - y \in T\) and \(xy \in T\). We can find \(r, s \in R\) such that \(x = rb\) and \(y = sb\). Then we have:

\[
x - y = (r - s)b \in T
\]
\[
xy = (xs)b \in T
\]

Thus \(T\) is a subring of \(R\).

*Problem 3.2.9.* First, \(S\) is not empty since it contains the zero matrix for instance. Let us show that \(S\) is closed under subtraction and multiplication. Let \(x, y \in S\), then we can write:

\[
x = \begin{pmatrix} a & 4b \\ b & a \end{pmatrix}
\]
\[
y = \begin{pmatrix} c & 4d \\ d & c \end{pmatrix}
\]

for some real numbers \(a, b, c, d\). Then we have:

\[
x - y = \begin{pmatrix} a & 4b \\ b & a \end{pmatrix} - \begin{pmatrix} c & 4d \\ d & c \end{pmatrix}
\]
\[
= \begin{pmatrix} a - c & 4(b - d) \\ b - d & a - c \end{pmatrix}
\]
so \( x - y \in S \). Also:

\[
xy = \begin{pmatrix} a & 4b \\ b & a \end{pmatrix} \begin{pmatrix} c & 4d \\ d & c \end{pmatrix} = \begin{pmatrix} ac + 4bd & 4(ad + bc) \\ bc + ad & 4bd + ac \end{pmatrix}
\]

thus \( xy \in S \). So \( S \) is a subring of \( M(R) \).

**Problem 3.2.13.** (a) Yes, \( S \cap T \) is a subring of \( R \). Proof: since \( S \) and \( T \) are subrings, they both contain 0. Thus \( 0 \in S \cap T \). Let us show the closure of \( S \cap T \) under subtraction and multiplication. Let \( x, y \in S \cap T \). Since \( S \) is a subring and \( x, y \in S \), we have \( x - y \in S \) and \( xy \in S \). Similarly, \( T \) is a subring and \( x, y \in T \) so \( x - y \in T \) and \( xy \in T \). Hence \( x - y \in S \cap T \) and \( xy \in S \cap T \). So \( S \cap T \) is a subring of \( R \).

(b) This is false. Counterexample: consider the two subrings of \( \mathbb{Z} \):

\[
2\mathbb{Z} = \{2n, n \in \mathbb{Z}\} \\
3\mathbb{Z} = \{3n, n \in \mathbb{Z}\}
\]

The fact that these are subrings of \( \mathbb{Z} \) follows from problem 3.2.8. Note that \( 2\mathbb{Z} \) (resp. \( 3\mathbb{Z} \)) is the set of integers divisible by 2 (resp. 3), so \( 2\mathbb{Z} \cup 3\mathbb{Z} \) is the set of integers divisible by either 2 or 3. Then \( 2\mathbb{Z} \cup 3\mathbb{Z} \) is not closed under addition. Indeed, \( 2 \in 2\mathbb{Z} \cup 3\mathbb{Z} \) and \( 3 \in 2\mathbb{Z} \cup 3\mathbb{Z} \), but \( 5 = 2 + 3 \) is not in \( 2\mathbb{Z} \cup 3\mathbb{Z} \) since it is divisible by neither 2 nor 3. In particular, \( 2\mathbb{Z} \cup 3\mathbb{Z} \) is not a subring of \( \mathbb{Z} \).

**Problem 3.2.14.** Let \( R \) be an integral domain and \( e \) be an idempotent of \( R \). Then we have \( e^2 = e \), which can be written \( e^2 - e = 0 \), or \( e(e - 1) = 0 \). Since \( R \) is an integral domain, we have \( e = 0 \) or \( e - 1 = 0 \), i.e. \( e = 0 \) or \( e = 1 \). Conversely, 0 and 1 are clearly idempotents of the ring \( R \). Thus the idempotents of \( R \) are precisely 0 and 1.

**Problem 3.2.19.** We claim that the units of \( R \times S \) are precisely the \( (r, s) \) with \( r \) a unit of \( R \) and \( s \) a unit of \( S \). Proof: first let \( r \) be a unit of \( R \) and \( s \) be a unit of \( S \), we prove that \( (r, s) \) is a unit of \( R \times S \). We have:

\[
(r, s)(r^{-1}, s^{-1}) = (rr^{-1}, ss^{-1}) = (1_R, 1_S) = 1_{R \times S}
\]

and similarly \( (r^{-1}, s^{-1})(r, s) = 1_{R \times S} \). Thus, \( (r, s) \) is a unit of \( R \times S \). Conversely, let \( (r, s) \) be a unit of \( R \times S \), we prove that \( r \) is a unit of \( R \) and \( s \) is a unit of \( S \). Since \( (r, s) \) is a unit of \( R \times S \), there exists \( (t, u) \in R \times S \) such that:

\[
(r, s)(t, u) = (t, u)(r, s) = 1_{R \times S} = (1_R, 1_S)
\]
Looking at the first component of this equality gives us $rt = tr = 1_R$. So $r$ is a unit of $R$. Looking at the second component gives $su = us = 1_S$. So $s$ is a unit of $S$. This proves the claim.

Problem 3.2.21. (a) Assume we have $ab = ac$ with $a, b, c \in R$ and $a$ non zero and not zero divisor. Then we have $ab - ac = 0$, i.e. $a(b - c) = 0$. Since $a$ is not a zero divisor, we have $b - c = 0$, so $b = c$.

(a) This is entirely similar: assume we have $ba = ca$ with $a, b, c \in R$ and $a$ non zero and not zero divisor. Then we have $ba - ca = 0$, i.e. $(b - c)a = 0$. Since $a$ is not a zero divisor, we have $b - c = 0$, so $b = c$.

Problem 3.2.38. Since $ab$ is a unit of $R$, there exists $u \in R$ such that $abu = uab = 1$. note that necessarily neither $a$ nor $b$ is zero. Let us prove that $a$ is a unit, with inverse $bu$. We have just seen that $a(bu) = 1$, we also need to check $(bu)a = 1$. If we multiply the equality $a(bu) = 1$ by $a$ on the right, we get $abua = a$. Since $a$ is not zero and not a zero divisor, we can apply the cancellation property seen in 3.2.21 (a) and we get $(bu)a = 1$, giving us that $a$ is a unit.

We prove entirely similarly that $b$ is a unit with inverse $ua$. We have seen above that $(ua)b = 1$, let us prove that we also have $b(ua) = 1$. If we multiply the equality $uab = 1$ with $b$ on the left, we get $buab = b$. Since $b$ is non zero and not a zero divisor, we can apply the property proved in 3.2.21 (b) and we get $b(ua) = 1$. So $b$ is a unit.

In conclusion, both $a$ and $b$ are units.

A few remarks. 1) If $R$ is a commutative ring, then the property holds without assuming that $a$ and $b$ are non zero divisors. Namely we have: for any $a, b \in R$, if $ab$ is a unit, then $a$ and $b$ are units. Indeed, the fact we have $abu = 1$ for some $u \in R$ implies that $bu = 1$ by commutativity, and thus $a$ is a unit with inverse $bu$. Similar reasoning applies to prove that $b$ is a unit with inverse $au$.

2) If $R = M_n(T)$ for some commutative ring $T$, the property also holds without assuming that $a$ and $b$ are non zero divisors. Namely, we have: for any $a, b \in M_n(T)$, if $ab$ is a unit, then $a$ and $b$ are units. Indeed, if we have $abu = 1$ in $M_n(T)$, we get the equality $\det(a)\det(b)\det(u) = 1$ in the commutative ring $T$. Thus, we get that $\det(a)$ and $\det(b)$ are units in the ring $T$. Hence, $a$ and $b$ are invertible matrices in $M_n(T)$.

3) So for our usual examples of rings, the property holds without assuming that $a$ and $b$ are non zero divisors. However, this fails in general without the requirement that $a$ and $b$ are not zero divisors. Let us give a counterexample. Consider the real vector space $V$ of real sequences. So elements of $V$ are sequences $u = (u_n)_{n \in \mathbb{N}}$ with $u_n \in R$. We can consider the ring $R = \text{End}(V)$ of linear endomorphisms of $V$. The multiplication in this ring is the composition of endomorphisms, and checking that $R$ is a ring is straightforward. In
this ring, the identity is the identity endomorphism, and an element is a unit if and only if it is a bijective linear transformation. Now consider the elements $a$ and $b$ of $R$ defined by:

\[
\begin{align*}
  a(u)_n &= u_{n+1} \\
  b(u)_n &= \begin{cases} 
    0 & \text{if } n = 0 \\
    u_{n-1} & \text{if } n \geq 1
  \end{cases}
\end{align*}
\]

for any $u \in V$. In words, $a$ shifts the sequence one unit to the left, while $b$ shifts the sequence one unit to the right and assigns the value 0 at 0. Then clearly $ab = 1$. However, $b$ is not a surjective map since any sequence that has a non zero value at 0 is not in the image of $b$. So $b$ is not a unit. Similarly, $a$ is not injective since any sequence that has a non zero value at 0 and 0 elsewhere will be in the kernel of $a$. So $a$ is not a unit either.