Solutions to Homework Set 3  
(Solutions to Homework Problems from Chapter 2)

Problems from §2.1

2.1.1. Prove that \( a \equiv b \pmod{n} \) if and only if \( a \) and \( b \) leave the same remainder when divided by \( n \).

Proof.

\( \Rightarrow \)

Suppose \( a \equiv b \pmod{n} \). Then, by definition, we have

\[
a - b = nk
\]

for some \( k \in \mathbb{Z} \). Now by the Division Algorithm, \( a \) and \( b \) can be written uniquely in form

\[
a = nq + r \\
b = nq' + r'
\]

with \( 0 \leq r, r' < n \). But then

\[
a = b + nk = (nq' + r') + nk = n(q' + k) + r'
\]

Comparing (??) and (??) we have

\[
a = nq + r \quad , \quad 0 \leq r < n \\
a = n(q' + k) + r' \quad , \quad 0 \leq r' < n
\]

By the uniqueness property of the division algorithm, we must therefore have \( r = r' \).

\( \Leftarrow \)

If \( a \) and \( b \) leave the same remainder when divided by \( n \) then we have

\[
a = nq + r \\
b = nq' + r
\]

Subtracting these two equations yields

\[
a - b = n(q - q')
\]

so

\[
a \equiv b \pmod{n}
\]

2.1.2. If \( a \in \mathbb{Z} \), prove that \( a^2 \) is not congruent to 2 modulo 4 or to 3 modulo 4.

- Proof.

  By the Division Algorithm any \( a \in \mathbb{Z} \) must have one of the following forms

\[
a = \begin{cases} 
4k \\
4k + 1 \\
4k + 2 \\
4k + 3 
\end{cases}
\]

This implies

\[
a^2 = \begin{cases} 
16k^2 = 4(4k^2) = 4q \\
16k^2 + 8k + 1 = 4(4k^2 + 2k) + 1 = 4r + 1 \\
4(4k^2 + 16k + 4) = 4(4k^2 + 8k + 1) = 4s \\
16k^2 + 24k + 9 = 4(4k^2 + 6k + 2) + 1 = 4t + 1 
\end{cases}
\]

\[1\]
So

\[ a^2 \equiv \begin{cases} 
0 \pmod{4} \\
1 \pmod{4} 
\end{cases} . \]

\[ \square \]

2.1.3. If \( a, b \) are integers such that \( a \equiv b \pmod{p} \) for every positive prime \( p \), prove that \( a = b \).

- **Proof.** Since the set of prime numbers in \( \mathbb{Z} \) is infinite, we can always find a prime number \( p \) larger than any given number. In particular we can find a prime number \( p \) such that

\[ 0 \leq |a - b| < p . \]

Now by hypothesis, we have, for this prime \( p \),

\[ a - b = kp \]

for some \( k \in \mathbb{Z} \) (by the definition of congruence modulo \( p \)). Thus, \( p \) divides \( |a - b| \). But 0 is the only non-negative number less than \( p \) that is also divisible by \( p \). Thus, \( |a - b| = 0 \) or \( a = b \). \( \square \)

2.1.4. Which of the following congruences have solutions:

(a) \( x^2 \equiv 1 \pmod{3} \)

- We need

\[ x^2 - 1 = 3k \]

By the Division Algorithm, \( x \) must have one of three forms

\[ x = \begin{cases} 
3t \\
3t + 1 \\
3t + 2 
\end{cases} \Rightarrow x^2 - 1 = \begin{cases} 
9t^2 - 1 \\
9t^2 + 6t \\
9t^2 + 12t + 3 
\end{cases} \]

Thus, if \( x \) has the form \( x = 3t + 1 \), then \( x^2 - 1 = 3(3t^2 + 2t) \) and so \( x^2 \equiv 1 \pmod{3} \). \( \square \)

(b) \( x^2 \equiv 2 \pmod{7} \)

- We need

\[ x^2 - 2 = 3k \]

By the Division Algorithm, \( x \) must have one of the seven forms

\[ x = \begin{cases} 
7k \\
7k + 1 \\
7k + 2 \\
7k + 3 \\
7k + 4 \\
7k + 5 \\
7k + 6 
\end{cases} \Rightarrow x^2 - 1 = \begin{cases} 
49k^2 - 2 \\
49k^2 + 14k - 1 \\
49k^2 + 28k + 2 \\
49k^2 + 42k + 7 \\
49k^2 + 70k + 14 \\
49k^2 + 70k + 23 \\
49k^2 + 84 + 34 
\end{cases} = \begin{cases} 
7k^2 + 2 \pmod{7} \\
7k^2 + 2k - 1 + 6 \pmod{7} \\
7k^2 + 4k + 2 \pmod{7} \\
7k^2 + 6k + 1 \pmod{7} \\
7k^2 + 8k + 2 \pmod{7} \\
7k^2 + 10k + 3 + 2 \pmod{7} \\
7k^2 + 12k + 4 + 6 \pmod{7} 
\end{cases} \]

Thus, if \( x \) has the form \( x = 7k + 3 \) or the form \( x = 7k + 4 \), then \( x^2 - 2 \) is an integer multiple of 7 and so \( x^2 \equiv 2 \pmod{7} \). \( \square \)

(c) \( x^2 \equiv 3 \pmod{11} \)

- This is best handled by trial and error. In order for \( x^2 \equiv 3 \pmod{11} \), we need

\[ x^2 - 3 = 11k \]

for some choice of integers \( x \) and \( k \). For \( x = 0, 1, 2, 3, 4 \) there is no such \( k \); but for \( x = 5 \) we have

\[ 5^2 - 3 = 22 = 2 \cdot 11 \cdot \]
so \( x = 5 \) is a solution. \( x = 6 \) is also a solution since
\[
6^2 - 3 = 33 = 3 \cdot 11 .
\]

2.1.5. If \([a] = [b] \) in \( \mathbb{Z}_n \), prove that \( \text{GCD}(a, n) = \text{GCD}(b, n) \).

- **Proof.**
  Since \([a] = [b] \), \( a \equiv b \pmod{n} \) by Theorem 2.3. But then by the definition of congruence modulo \( n \)
  \[
a - b = nk
\]
  for some \( k \in \mathbb{Z} \). But this implies
  \[
a = nk + b .
\]
  Now we apply Lemma 1.7 (if \( x, y, q, r \in \mathbb{Z} \) and \( x = yq + r \), then \( \text{GCD}(x, y) = \text{GCD}(y, r) \)) taking
  \( x = a \) and \( y = n \). Thus,
  \[
  \text{GCD}(a, n) = \text{GCD}(n, b) .
  \]

2.1.6. If \( \text{GCD}(a, n) = 1 \), prove that there is an integer \( b \) such that \( ab \equiv 1 \pmod{n} \).

- **Proof.**
  Since \( \text{GCD}(a, n) = 1 \), we know by Theorem 1.3 that there exist integers \( u \) and \( v \) such that
  \[
  au + nv = 1 .
  \]
  Hence
  \[
  au - 1 = -nv .
  \]
  If we now set \( b = u \) and \( k = -v \) we have
  \[
  ab - 1 = nk
  \]
  which means that \( ab \equiv 1 \pmod{n} \). □

2.1.7. Prove that if \( p \geq 5 \) and \( p \) is prime then either \([p]_6 = [1]_6 \) or \([p]_6 = [5]_6 \).

- Let \( p \) be a prime \( \geq 5 \). Then \( p \) is not divisible by 2 or 3. Now consider the \textit{a priori} possible
  congruency classes of \([p]_6 \); viz.,

  \[
  \mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6 \}
  \]
  one by one. \([p]_6 \) cannot be \([0]_6 \) since \( p \) is not divisible by 6. For
  \( p \in [0]_6 \implies p \equiv 0 \pmod{6} \implies p - 0 = k6 \) for some \( k \in \mathbb{Z} \implies 6 \mid p \) (contradiction!)
  Similarly,

  \[
  p - 2 = k6 \implies p = k6 - 2 = 2(3k - 1) \implies 2 \mid p \) (contradiction!)
  \]
  \( p \in [2]_6 \implies p - 3 = k'6 \implies p = 3(2k' - 1) \implies 3 \mid p \) (contradiction!)
  and

  \[
  p \in [4]_6 \implies p - 4 = k''6 \implies p = 2(2k'' - 2) \implies 2 \mid p \) (contradiction!)
  
  The only possibilities left are \([p]_6 = [1]_6 \) and \([p]_6 = [5]_6 \). □
Problems from §2.2

2.2.1. Write out the addition and multiplication tables for $\mathbb{Z}_4$.

Addition in $\mathbb{Z}_4$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Multiplication in $\mathbb{Z}_4$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

2.2.2. Prove or disprove: If $ab = 0$ in $\mathbb{Z}_n$, then $a = 0$ or $b = 0$.

- **Disproof by Counter-Example**

2.2.3 Prove that if $p$ is prime then the only solutions of $x^2 + x = 0$ in $\mathbb{Z}_p$ are 0 and $p-1$.

- **Proof.**
  Let us revert to the original explicit notation for elements of $\mathbb{Z}_p$. We want to prove

$$([x] \odot [x]) \oplus [x] = [0] \quad (\text{in } \mathbb{Z}_p) \quad \Rightarrow \quad [x] = [0] \text{ or } [p-1].$$

Now, by the definition of addition and multiplication in $\mathbb{Z}_p$, statement (??) is equivalent to

$$[x(x-1)] = [0] \quad \Rightarrow \quad [x] = [0] \text{ or } [p-1].$$

Now if the congruence class in $\mathbb{Z}_p$ of $x^2 + x$ is the same as that of 0, then the difference between $x^2 + x$ and 0 must be divisible by $p$. Hence, $p$ divides $x^2 + x = 0 = x^2 + x$. Now

$$x^2 + x = x(x+1).$$

Since $p$ is prime, and $p$ divides $x(x+1)$, $p$ must divide either $x$ or $x+1$ (by Corollary 1.9). If $p$ divides $x$, then $qp = x = x - 0$ so $x$ is in the same congruence class as 0; i.e., $[x] = [0]$. If $p$ does not divide $x$, then it must divide $x + 1$; so

$$x + 1 = q'p$$

$$\Rightarrow [x] = [-1] = [p-1].$$

2.2.4. Find all $[a]$ in $\mathbb{Z}_5$ for which the equation $ax = 1$ has a solution.

- **Let us write down the multiplication table for $\mathbb{Z}_5$.**
2.2.5. Prove that there is no ordering \( \prec \) of \( \mathbb{Z}_n \) such that

\[
\begin{align*}
(i) & \quad \text{if } a \prec b, \text{ and } b \prec c, \text{ then } a \prec c; \\
(ii) & \quad \text{if } a \prec b, \text{ then } a + c \prec b + c \text{ for every } c \in \mathbb{Z}_n.
\end{align*}
\]

- **Proof.**

By an ordering on \( \mathbb{Z}_n \) we mean a rule that tells you whether or not pairs of elements of \( \mathbb{Z}_n \).

In addition to the conditions given above, we must assume that the ordering is *complete* in the sense that if \( a \neq b \) then either \( a \prec b \) or \( b \prec a \).

So assume we have such a relation on \( \mathbb{Z}_n \). Since \([0]\) and \([1]\) are distinct congugacy classes in \( \mathbb{Z}_n \),
we must then have either \([0] \prec [1]\) or \([1] \prec [0]\).

Assume \([0] \prec [1]\). Then by property (ii) we must have

\[
[0] + [c] \prec [1] + [c], \quad \forall [c] \in \mathbb{Z}_n.
\]

Since \([0] + [c] = [c]\) and \([1] + [c] = [c + 1]\), we then have

\[
[c] \prec [c + 1], \quad \forall [c] \in \mathbb{Z}_n.
\]

Thus,

\[
[0] \prec [1] \prec [2] \prec \cdots \prec [n - 1] \prec [n] \prec [n + 1] \cdots.
\]

Applying Property (i) recursively,

\[
\begin{align*}
\end{align*}
\]

etc.,

we can conclude that \([1] \prec [n]\). But \([n] = [0]\) in \( \mathbb{Z}_n \). So \([1] \prec [0]\). But this contradicts our assumption that \([0] \prec [1]\). Hence no such ordering exists.

The case when \([1] \prec [0]\) is treated similarly. \(\square\)

Problems from §2.3

2.3.1 If \( n \) is composite, prove that there exists \( a, b \in \mathbb{Z}_n \) such that \( a \neq [0] \) and \( b \neq [0] \) but \( ab = [0] \).

- **Proof.**

Assume \( n \) to be positive (otherwise, we have to define \( \mathbb{Z}_n \) for \( n < 0 \); which can be done, but with no particular gain). If \( n \) is composite then \( n \) has a factorization

\[
n = pq
\]
with
\[ 1 < p \leq q < n \ . \]

In view of the inequality above \( n \) does not divide \( p \) nor does \( n \) divide \( q \), so
\[ [p] \neq [0] \quad \text{and} \quad [q] \neq [0] . \]

However,
\[ [p][q] = [pq] = [n] = [0] . \]

Setting \( a = [p] \) and \( b = [q] \) we arrive at the desired conclusion. □

2.3.2 Let \( p \) be prime and assume that \( a \neq 0 \) in \( \mathbb{Z}_p \). Prove that for any \( b \in \mathbb{Z}_p \), the equation \( ax = b \) has a solution.

\[ \boxed{\text{Proof.}} \]

By Theorem 2.8, the equation \( ax' = 1 \) always has a solution in \( \mathbb{Z}_p \), for every \( a \neq [0] \) if \( p \) is prime. Multiplying both sides by \( b \in \mathbb{Z}_p \), yields
\[ bax' = b \]

Setting \( x = bx' \) we see that every \( b \in \mathbb{Z}_p \) has a factorization
\[ b = ax \]

for every \( [a] \neq [0] \) in \( \mathbb{Z}_p \). □

2.3.3. Let \( a \neq [0] \) in \( \mathbb{Z}_n \). Prove that \( ax = [0] \) has a nonzero solution in \( \mathbb{Z}_n \) if and only if \( ax = [1] \) has no solution.

\[ \boxed{\text{Proof.}} \]

\( \Rightarrow \)
Suppose \( a \neq [0] \), \( b \neq [0] \) and that \( ab = [0] \). We aim to show that \( ax = [1] \) has no solution. We will use a proof by contradiction. Suppose \( c \) is a solution of \( ax = [1] \). Then
\[ b = b \cdot 1 = b(ac) = (ab)c = [0] \cdot c = 0 \ . \]

But this contradicts our original hypothesis that \( b \) is a \textbf{nonzero} solution of \( ax = [0] \). Hence, there can be no solution of \( ax = [1] \).

\( \Leftarrow \)
Suppose \( a \neq [0] \) and \( ax = [1] \) has no solution. We aim to show that \( ax = [0] \) has a nonzero solution in \( \mathbb{Z}_n \). Let \( z \) be the integer, lying between 1 and \( n - 1 \) representing the congruence class of \( a \in \mathbb{Z}_n \); i.e.,
\[ [z] = a . \]

We first note that, by Corollary 2.9, \( \gcd(z, n) = 1 \) if and only if \( ax = [1] \) has a solution in \( \mathbb{Z}_n \). Since the latter is not so, \( \gcd(z, n) \neq 1 \) and so \( z \) and \( n \) must share a common divisor greater than 1, call it \( t \). We thus have
\[ z = rt \quad , \quad n = st \ . \]

By construction \( 1 \leq s < n \), and so the congruence class of \( s \) is not equal to \( [0] \). But
\[ a[s] = [z][s] = [rt][s] = [r][st] = [r][0] = [0] . \]

Hence, \( [s] \) is a nonzero solution of \( ax = [0] \) in \( \mathbb{Z}_n \). □

2.3.4. Solve the following equations.
(a) \( 12x = 2 \) in \( \mathbb{Z}_{19} \).
• The fastest approach to this problem might be trial and error. Simply compute the multiples $0 \cdot 12$, $1 \cdot 12$, $\ldots$, $18 \cdot 12$ and figure out which of these products have remainder 2 when divided by 19. Then we’d have

$$k \cdot 12 = q \cdot 19 + 2$$

or

$$2 \equiv k \cdot 12 \pmod{19}$$

and so

$$[12]_{19} [k]_{19} = [2]_{19}$$

hence the solution of

$$[12]_{19} x = [2]_{19}$$

will be $[k]_{19}$. Such a trial and error procedure reveals

$$192 = (10)(19) + 2 \Rightarrow [12]_{19} [16]_{19} = [2]_{19} \Rightarrow x = [16]_{19}$$

• Next, we give a more systematic approach which is also applicable for large integers (where the trial and error procedure because tedious if not impractical). Apply the Euclidean Algorithm to the pair $(19, 12)$.

$$19 = (1) (12) + 7$$
$$12 = (1) (7) + 5$$
$$7 = (1) (5) + 2$$
$$5 = (2) (2) + 1$$
$$1 = (1) (1) + 0$$

The point here is not to figure out the GCD of 19 and 12 (which is obviously 1 since 19 is prime), but to obtain a useful arrangement of substitutions what will allows us to express 1 as an integer linear combination of 19 and 12. That is to find numbers $u$ and $v$ so that

$$1 = u (19) + v (12)$$

The utility of this equation well become clear once we get a suitable choice of $v$ and $u$.

We re-write the sequence of Euclidean Algorithm equations so the remainders are isolated on the left hand side

$$1 = 5 - (2)(2) \quad \text{(a)}$$
$$2 = 7 - (1)(5) = 7 - 5 \quad \text{(b)}$$
$$5 = 12 - (1)(7) = 12 - 7 \quad \text{(c)}$$
$$7 = 19 - (1)(12) = 19 - 12 \quad \text{(d)}$$

Now the idea is to use back substitution to eliminate all the intermediary remainders: substituting the right hand side of (d) for the number 7 in (c) yields

$$5 = 12 - (19 - 12) = (2)(12) - 19 \quad \text{(e)}$$

We’ve now expressed 7 and 5 in the form $12u + 19v$. Substituting the right hands sides of (d) and (e) into (b) yields

$$2 = (19 - 12) - ((2)(12) - 19) = (2)(19) - (3)(12) \quad \text{(f)}$$

Finally, we substitute the right hands sides of (e) and (f) into (a) to get

$$1 = ((2)(12) - 19) - 2((2)(19) - (3)(12)) = (-5)(19) + (8)(12)$$

The last equality just being a check on our calculation. We now have

$$(12)(8) - (5)(19) = 1$$

Taking congruence classes of both sides modulo 19 we get

$$[12]_{19} [8]_{19} - [5]_{19} [19]_{19} = [1]_{19}$$

or since $[19]_{19} = 0$,

$$[12]_{19} [8]_{19} = [1]_{19}$$
Now simply multiply both sides by \([2]_{19}\), to obtain

\[ [2]_{19} [12]_{19} [8]_{19} = [2]_{19} [1]_{19} \]

or using \([2]_{19} [8]_{19} = [16]_{19}\), and \([2]_{19} [1]_{19} = [2]_{19}\)

\[ [12]_{19} [16]_{19} = [2]_{19} \]

Thus,

\[ X = [16]_{19} \]

is the solution to

\[ [12]_{19} X = [2]_{19} \].

\(\square\)

(b) 7\(x\) = 2 in \(\mathbb{Z}_{24}\).

- Either method used in part (a) will produce

\[ (7) (14) = 98 = (4) (24) + 2 \quad \Rightarrow \quad [7]_{24} [14]_{24} = [2]_{24} \quad \Rightarrow \quad x = [14]_{24} \]

\(\square\)

(c) 31\(x\) = 1 in \(\mathbb{Z}_{50}\).

- Either method used in part (a) will produce

\[ (31)(20) = 651 = (7)(50) + 1 \quad \Rightarrow \quad [31]_{50} [20]_{50} = [1]_{50} \quad \Rightarrow \quad x = [20]_{50} \]

\(\square\)

(d) 34\(x\) = 1 in \(\mathbb{Z}_{97}\).

- Here only the second method of part (a) is actually practical. We’ll do the calculation explicitly. First we apply the Euclidean algorithm to the pair (97,34).

\[
\begin{align*}
97 &= (2)(34) + 29 \\
34 &= (1)(29) + 5 \\
29 &= (5)(5) + 4 \\
5 &= (1)(4) + 1
\end{align*}
\]

Now we back-substitute to express 1 as an integer linear combination of 97 and 34. We have

\[
\begin{align*}
1 &= 5 - (1)(4) \\
4 &= 29 - (5)(5) & \text{(b)} \\
5 &= 34 - (1)(29) & \text{(c)} \\
29 &= 97 - (2)(34) \quad & \text{(d)}
\end{align*}
\]

and so

\[
\begin{align*}
29 &= 1 \cdot 97 - 2 \cdot 34 \\
5 &= 34 - 1 \cdot 29 = 34 - (1 \cdot 97 - 2 \cdot 34) = -97 + 3 \cdot 34 \\
4 &= 29 - 5 \cdot 5 = (97 - 2 \cdot 34) - 5(-97 + 3 \cdot 34) = 6 \cdot 97 - 17 \cdot 34 \\
1 &= 5 - 4 = (-97 + 3 \cdot 34) - (6 \cdot 97 - 17 \cdot 34) \\
&\quad = -7 \cdot 97 + 20 \cdot 34
\end{align*}
\]

or

\[ 20 \cdot 34 - 7 \cdot 97 = 1 \]
So \[ 1 \equiv (20) (34) \pmod{97} \]

so \[ [34]_{97} [20]_{97} = [1]_{97} \]

and so \([20]_{97}\) is the solution of \[ [34]_{97} X = [1]_{97} \]