Homework set 8 – Solutions
Math 310 – Renato Feres

Note 1. Work on all the problems listed below, but only those marked with an (*) need to be turned in.
Note 2. The problems marked with (*) are all worth the same number of points.
Note 3. Chapters and exercise numbers refer to the 4th edition of Liebeck's text.

⋄ 1. Read Chapters 12 and 13 of Liebeck's textbook.

2. Chapter 12, Exercise 3 (*) For a positive integer \( n \), define \( \varphi(n) \) to be the number of positive integers \( a < n \) such that \( \text{hcf}(a, n) = 1 \). (For example, \( \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2 \).)

(a) Work out \( \varphi(n) \) for \( n = 5, 6, \ldots, 10 \).

(b) If \( p \) is a prime, show that \( \varphi(p) = p - 1 \) and, more generally, that \( \varphi(p^r) = p^r - p^{r-1} \).

Solution.

(a) The set \( S(n) \) of positive integers \( a < n \) coprime with \( n \), and the values of \( \varphi(n) \) are as follows.

i. \( S(5) = \{1, 2, 3, 4\}, \varphi(5) = 4; \)

ii. \( S(6) = \{1, 5\}, \varphi(6) = 2; \)

iii. \( S(7) = \{1, 2, 3, 4, 5, 6\}, \varphi(7) = 6; \)

iv. \( S(8) = \{1, 3, 4, 7\}, \varphi(8) = 4; \)

v. \( S(9) = \{1, 2, 4, 5, 7, 8\}, \varphi(9) = 6; \)

vi. \( S(10) = \{1, 3, 7, 9\}, \varphi(10) = 4. \)

(b) Let us prove the general case \( r \geq 1 \). Clearly, the case \( \varphi(p) = p - 1 \) will follow. Let \( S \) denote the set of integers between 1 and \( p^r \), including these two numbers. \( S \) has, clearly, \( p^r \). An element \( a \in S \) satisfies \( \text{hcf}(a, p^r) \neq 1 \) if and only if \( a = pm \), for some integer \( m \). This is because \( p \) is the only prime factor of \( p^r \), hence \( \text{hcf}(a, p^r) = 1 \) if and only if \( a \) does not contain \( p \) as a prime factor. Therefore the set difference \( S \setminus R \) (the subset of elements of \( S \) not in \( R \)), where \( R = \{p, 2p, \ldots, p^{r-1}p\} \), consists of positive integers \( m < p^r \) coprime with \( p^r \). But this set difference has exactly \( p^r - p^{r-1} \) elements.

⋄

3. Chapter 13, Exercise 2 (*) Let \( p \) be a prime number and \( k \) a positive integer.

(a) Show that if \( x \) is an integer such that \( x^2 \equiv x \mod p \), then \( x \equiv 0 \) or \( 1 \mod p \).

(b) Show that if \( x \) is an integer such that \( x^2 \equiv x \mod p^k \), then \( x \equiv 0 \) or \( 1 \mod p^k \).
Solution.

(a) Clearly, this part of the exercise follows from the more general statement of the second part. We prove the general case next.

(b) The equation $x^2 \equiv x \mod p^k$ is equivalent to $p^k$ dividing $x^2 - x$. Note that $x^2 - x = x(x - 1)$ and that $x, x - 1$ are coprime to each other. Therefore $p^k$ dividing $x(x - 1)$ implies $p^k$ divides $x$ or $x - 1$. If $p^k$ divides $x$ then $x \equiv 0 \mod p^k$, and if $p$ divides $x - 1$ then $x \equiv 1 \mod p^k$.

⋄

4. Chapter 13, Exercise 3 (∗) For each of the following congruence equations, either find a solution $x \in \mathbb{Z}$ or show that no solution exists:

(a) $99x \equiv 18 \mod 30$
(b) $91x \equiv 84 \mod 143$
(c) $x^2 \equiv 2 \mod 5$
(d) $x^2 + x + 1 \equiv 0 \mod 5$
(e) $x^2 + x + 1 \equiv 0 \mod 7$

Solution. According to Proposition 13.6, the congruence equation $ax \equiv b \mod m$ has a solution $x \in \mathbb{Z}$ if and only if $\text{hcf}(a, m)$ divides $b$.

(a) A calculation gives $\text{hcf}(99, 30) = 3$ and 3 divides 18, so a solution must exist. To solve the equation, first observe that the equation is equivalent to $99x - 18 = 30k$ for some integer $k$, which is equivalent (upon dividing by 3) to $33x - 6 = 10k$. Since 33 and 10 are coprime to each other, there are integers $r$ and $s$ such that $33r + 10s = 1$. In fact, take $r = -3$ and $s = 10$. Thus $33 \times (-3) = 1 - 10 \times 10$. Multiplying the equation $33x \equiv 6 \mod 10$ by $-3$ gives

$$6 \times (-3) = 33 \times (-3)x \equiv x - 100x \equiv x \mod 10.$$ we conclude that $x = -18$ (or $x = 2$) satisfies the equation.

(b) A calculation gives $\text{hcf}(91, 143) = 13$, and 13 does not divide 84, a solution cannot exist.

(c) There are only 5 possible values of $x$ modulo 5: 0, 1, 2, 3, 4. Their squares are 0, 1, 4, 9 ≡ 4 mod 5 and 16 ≡ 1 mod 5. Thus there is no value of $x$ whose square is congruent to 2 modulo 5.

(d) As in the previous item, we compute the values modulo 5 of $f(x) = x^2 + x + 1$ for $x = 0, 1, 2, 3, 4$. We see $f(0) = 1$, $f(1) = 3$, $f(2) = 7$, $f(3) = 13$, $f(4) = 21$. In all cases $f(x)$ is not divisible by 5, so there are no solutions.

(e) We see that $f(2) = 7$ and $f(4) = 21$, so 2, 4 are solutions modulo 7. There are no other solutions.

⋄

5. Chapter 13, Exercise 6 (∗) Let $p$ be a prime number, and let $a$ be an integer that is not divisible by $p$. Prove that the congruence equation $ax \equiv 1 \mod p$ has a solution $x \in \mathbb{Z}$.

Solution. Since $p$ does not divide $a$, the highest common divisor of $p$ and $a$ is 1. Thus there are integers $r, s$ such that $pr + as = 1$, from which it follows that $as \equiv 1 \mod p$. We conclude that $x = s$ is a solution.
6. **Chapter 13, Exercise 9.** Let \( p \) be a prime and let \( \overline{a}, \overline{b} \in \mathbb{Z}_p \), with \( \overline{a} \neq 0 \). Prove that the equation \( \overline{a}x = \overline{b} \) has a solution for \( \overline{x} \in \mathbb{Z}_p \).

**Solution.** We just showed in (5) that the equation \( \overline{a}y = 1 \) has a solution. Then \( x = \overline{b}y \) is a solution of \( \overline{a}x = \overline{b} \).

7. **Chapter 13, Exercise 10 (**) 

   (a) Construct the addition and multiplication tables for \( \mathbb{Z}_6 \).

   (b) Find all solutions in \( \mathbb{Z}_6 \) of the equation \( \overline{x}^2 + \overline{x} = 0 \).

**Solution.**

(a) To simplify the notation, I omit the bar indicating congruence class. The table for addition is

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

The table for multiplication is

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<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>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

(b) Substituting each of the possible 5 values of \( \overline{x} \) into \( \overline{x}^2 + \overline{x} \) shows that \( x = 0, 2, 3, 5 \) are all solutions modulo 6.