CPS102 hw2 solutions and hints

February 12, 2007

hw2a: 2.1 - 8

Solution  We will try to solve equation

\[ 487 \cdot_{30031} x = 13008 \]

let \( a = 487, b = 13008, n = 30031 \), we have to solve equation

\[ a \cdot_{n} x = b \]

Let \( a' \) be the multiplicative inverse of \( a \) in \( \mathbb{Z}_n \), and then we will have \( x = a' \cdot_{n} b \). Finding \( a' \) is hard by hand, however we can find \( a' \) using Euclid’s extended GCD algorithm. We need to compute \( \text{Inverse}(a, n) \) where \( a = 487 \) and \( n = 30031 \) in order to find \( x' \) and \( y' \). We use the following table to represent the computation process of the \( \text{Inverse} \) function:

<table>
<thead>
<tr>
<th>j</th>
<th>k</th>
<th>q</th>
<th>r</th>
<th>x'</th>
<th>y'</th>
</tr>
</thead>
<tbody>
<tr>
<td>487</td>
<td>30031</td>
<td>61</td>
<td>324</td>
<td>-14923</td>
<td>242</td>
</tr>
<tr>
<td>324</td>
<td>487</td>
<td>1</td>
<td>163</td>
<td>242</td>
<td>-161</td>
</tr>
<tr>
<td>163</td>
<td>324</td>
<td>1</td>
<td>161</td>
<td>-161</td>
<td>81</td>
</tr>
<tr>
<td>161</td>
<td>163</td>
<td>1</td>
<td>2</td>
<td>81</td>
<td>-80</td>
</tr>
<tr>
<td>2</td>
<td>161</td>
<td>80</td>
<td>1</td>
<td>-80</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Therefore, \( x' = -14923 \), therefore the inverse of \( a \) is \( x' \mod n = 15108 \). Then we have

\[
x = a' \cdot_n b = 15108 \cdot 30031 \cdot 13008 = 2000
\]

**hw2a: 2.1 - 12 (a)**

**Solution** Prove that \( a \cdot_p b \) are all different for \( b \) runs through 0 to \( p - 1 \). Prove by contradiction. Assume there exist \( b_1 \) and \( b_2 \) in \([0..p - 1]\) such that \( b_1 \neq b_2 \) and

\[
a \cdot_p b_1 = a \cdot_p b_2
\]

Since \( b_1 \neq b_2 \), we have \( a \cdot b_1 \neq a \cdot b_2 \), then there exist \( k_1 \neq k_2 \) such that

\[
a \cdot b_1 = k_1 p + r
\]

and

\[
a \cdot b_2 = k_2 p + r
\]

for \( 0 \leq r < p \). We then have \( a(b_1 - b_2) = (k_1 - k_2)p \) where \( k_1 - k_2 \neq 0 \) and \( b_1 - b_2 \neq 0 \). Since \( 1 \leq a \leq p - 1 \), then \( p \) does not divide \( a \). Then \( p \) must divide \( b_1 - b_2 \) therefore \( p \) must divide \( |b_1 - b_2| \). Since \( 0 \leq b_1 \leq p - 1 \) and \( 0 \leq b_2 \leq p - 1 \), then \( |b_1 - b_2| < p \). The \( p \) does not divide \( |b_1 - b_2| < p \). Contradiction. Therefore the products \( a \cdot_p b \) are all different.

**hw2b: 2.2 -2**

**Solution** Yes. \( 133 \mod n \).

**hw2b: 2.2 - 14**

**Hints** According to the extended GCD algorithm, a number \( a \) in \( \mathbb{Z}_n \) does not have a multiplicative inverse in \( \mathbb{Z}_n \) if \( \text{GCD}(a, n) \neq 1 \). Therefore, the answers are all the factors of 35 except 1.
hw2c: 2.2 - 12

Solution Since $gcd(16, 103) = 1$, the inverse exists. Apply the Euclid’s extended GCD algorithm to find the inverse by running function $Inverse(a, n)$ where $a = 16$ and $n = 103$.

The details of the extended algorithm are shown as follows:

<table>
<thead>
<tr>
<th>j</th>
<th>k</th>
<th>q</th>
<th>r</th>
<th>x</th>
<th>y</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>103</td>
<td>6</td>
<td>7</td>
<td>-45</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>16</td>
<td>2</td>
<td>2</td>
<td>7</td>
<td>-3</td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td>3</td>
<td>1</td>
<td>-3</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>/</td>
<td>0</td>
</tr>
</tbody>
</table>

Therefore $x = -45$, the inverse is $x \mod n = -45 \mod 103 = 58$.

hw2c: 2.2 - 22

Hints To prove that $a \cdot_n x = b$ has a unique solution in $\mathbb{Z}_n$ then $gcd(a, n) = 1$. This is the same as proving that if $gcd(a, n) > 1$ then the inverse of $a \mod n$ does not exist.

Let $a'$ be the inverse of $a \mod n$, then by definition $a' \cdot a - 1 = kn$ for some integer $k$. If $a$ and $n$ both have a divisor $p > 1$, then 1 has the same divisor $p > 1$ since $1 = a'a - kn$, contradiction.

hw2d: 2.3 -2

Solution Yes. Yes.
Hints (b) prove that i) reflexive:

\[ x \equiv x \pmod{n} \]

ii) symmetric: if \( x \equiv y \pmod{n} \) then \( y \equiv x \pmod{n} \)

iii) transitive: if \( x \equiv y \pmod{n} \) and \( y \equiv z \pmod{n} \) then \( x \equiv z \pmod{n} \)

c) express the equations in the theorem by

\[ x \equiv a \pmod{m} \]

and

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

**Remark**

You might get points off for not explaining the formula you used. Please talk to me if you have questions regarding your homework / grading.