Introduction to Cryptography

2008 Fall
Assignment 1 solution
Chapter 3 Exercise

1. 1, p: 104
   a) Find integers x and y such that $17x + 101y = 1$.
   b) Find $17^{-1} \pmod{101}$.

Sol.
   a) Use extended Euclidean algorithm.
   b) Use the result of a).
Sol. (con.)

a) \[
\begin{array}{c|c|c|c}
  & 101 & 17 & 1 \\
 5 & 101 & 17 & 1 \\
 85 & 16 & 1 \\
 16 & 1 & 1 \\
\end{array}
\]

\[
\Rightarrow q_1 = 5, \quad q_2 = 1,
\]

\[
\Rightarrow x_0 = 0, \quad x_1 = 1, \quad x_2 = -q_2 x_1 + x_0 = -1,
\]

\[
y_0 = 1, \quad y_1 = -q_1 = -5, \quad y_2 = -q_2 y_1 + y_0 = 6.
\]

\[
\Rightarrow (x, y) = (-1, 6). \quad [101 \cdot (-1) + 17 \cdot 6 = 1]
\]

b) For \(101 \cdot (-1) + 17 \cdot 6 = 1\)

\[
\Rightarrow 17 \cdot 6 \equiv 1 \mod 101
\]

\[
\Rightarrow 17^{-1} \equiv 6 \mod 101.
\]
Chapter 3 Exercise

2. 3, p: 104
   a) Find all solutions of $12x \equiv 28 \pmod{236}$.
   b) Find all solutions of $12x \equiv 30 \pmod{236}$.

Sol.
   a) $12x \equiv 28 \pmod{236}$
      $\Rightarrow \gcd(12, 236) = 4$,
      $\Rightarrow 3x \equiv 7 \pmod{59}$, solve $x \equiv 22 \pmod{59}$
      $\Rightarrow x \equiv 22, 81, 140, 199 \pmod{236}$. 
Sol. (con.)

b) \[ 12x \equiv 30 \pmod{236} \]

\[ \Rightarrow \gcd(12, 236) = 4, \]

\[ \Rightarrow \text{but 4 does not divide 30,} \]

\[ \Rightarrow \text{no solution.} \]
A group of people are arranging themselves for a parade. If they line up three to a raw, one person is left over. If they line up four to a raw, two people are left over, and if they line up five to a raw, three people are left over. What is the smallest possible number of people? What is the next smallest number? (Hint: Interpret this problem in terms of the CRT.)
Sol.

Use CRT:

\[
\begin{cases}
x \equiv 1 \mod 3 \\
x \equiv 2 \mod 4 \\
x \equiv 3 \mod 5
\end{cases}
\]

\[\Rightarrow x \equiv 58 \mod 60\]

\[\Rightarrow \text{The smallest possible \# of people is 58}\]

\[\text{The next smallest possible \# of people is 118.}\]
Chapter 3 Exercise

4. 25, p: 108

a) Find all four solutions to $x^2 \equiv 133 \pmod{143}$. (Note that $143 = 11 \cdot 13$.)

b) Find all solutions to $x^2 \equiv 77 \pmod{401}$. (There are only two solutions in this case. This is because $\gcd(77, 143) \neq 1$.)
Sol.

a) Consider $x^2 \equiv 133 \pmod{143}$

\[
\begin{align*}
    x^2 &\equiv 133 \equiv 1 \pmod{11} \\
    x^2 &\equiv 133 \equiv 3 \pmod{13}
\end{align*}
\]

$\Rightarrow$  $x \equiv \pm 1 \pmod{11}$

$\Rightarrow$  $x \equiv \pm 4 \pmod{13}$

$\Rightarrow$  $x \equiv 56, 100, 43, 87 \pmod{143}$.

b) Consider $x^2 \equiv 77 \pmod{143}$

\[
\begin{align*}
    x^2 &\equiv 77 \equiv 0 \pmod{11} \\
    x^2 &\equiv 77 \equiv 12 \pmod{13}
\end{align*}
\]

$\Rightarrow$  $x \equiv 0 \pmod{11}$

$\Rightarrow$  $x \equiv \pm 5 \pmod{13}$

$\Rightarrow$  $x \equiv 44, 99 \pmod{143}$.
Chapter 3 Exercise

5. 29, p: 109

Use the Legendre symbol to determine which of the following congruences have solutions (each modulus is prime):

a) \( X^2 \equiv 123 \) (mod 401)

b) \( X^2 \equiv 43 \) (mod 179)

c) \( X^2 \equiv 1093 \) (mod 65537)
Sol.

Compute the Legendre symbol:

a) \[ \left( \frac{123}{401} \right) = \left( \frac{3}{401} \right) \left( \frac{41}{401} \right) = \left( \frac{401}{3} \right) \left( \frac{401}{41} \right) = \left( \frac{2}{3} \right) \left( \frac{32}{41} \right) \]

\[ = -1 \times \left( \frac{2}{41} \right) \left( \frac{16}{41} \right) = -1 \times \left( \frac{2}{41} \right) = -1 \]

\[ \Rightarrow X^2 \equiv 123 \ (\text{mod} \ 401) \text{ has no solution.} \]
Sol. (con.)

Compute the Legendre symbol:

\[
b) \left(\frac{43}{179}\right) = -1 \times \left(\frac{179}{43}\right) = -\left(\frac{7}{43}\right) = -\left(-1 \times \left(\frac{43}{7}\right)\right) = \left(\frac{1}{7}\right) = 1
\]

\[
\Rightarrow X^2 \equiv 43 \pmod{179} \text{ has a solution.}
\]
Sol. (con.)
Compute the Legendre symbol:

c) \( \left( \frac{1093}{65537} \right) = \left( \frac{65537}{1093} \right) = \left( \frac{1050}{1093} \right) \)

\[ = \left( \frac{2}{1093} \right) \left( \frac{3}{1093} \right) \left( \frac{5^2}{1093} \right) \left( \frac{7}{1093} \right) \]

\[ = -1 \times \left( \frac{1093}{3} \right) \left( \frac{1093}{7} \right) = -\left( \frac{1}{3} \right) \left( \frac{1}{7} \right) = -1 \]

\[ \Rightarrow X^2 \equiv 1093 \pmod{65537} \text{ has no solution.} \]
6. The powers of 3 (mod 29) are 3, 9, 27, 23, 11, 4, 12, 7, 21, 5, 15, 16, 19, 28, 26, 20, 2, 6, 18, 25, 17, 22, 8, 24, 14, 13, 10, 1, so 3 is a generator for $\mathbb{Z}_{29}^\ast$.

a) Find all generators in $\mathbb{Z}_{29}^\ast$? (Actually you don't need to calculate all $g^x$'s to test if $g$ is a generator. Think about it!)

b) In general, how many generators in $\mathbb{Z}_p^\ast$ for a prime $p$?
Sol.

a) Find all $x$ such that $\gcd(x, 28) = 1$, then $3x$ must also be a generator for $\mathbb{Z}_{29}^\ast$.

$\Rightarrow x = 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27$

$\Rightarrow$ The generators for $\mathbb{Z}_{29}^\ast$ are $3, 27, 11, 21, 15, 19, 26, 2, 18, 8, 14, 10$.

b) Observe the result of a), we find all $x$ such that $\gcd(x, p-1) = 1$, so there are $\varphi(p-1)$ generators in $\mathbb{Z}_p^\ast$ for a prime $p$. 
7.
   a) Why is $Z_4 = \{0, 1, 2, 3\}$ not a field?
   b) Describe a finite field of 4 elements.
   c) Describe a finite field of 9 elements and indicate the multiplicative inverse of each nonzero element. (You may use \( h(x) = x^2 + 1 \) as your irreducible polynomial.)
Sol.

a) We can find that 2 has no multiplicative inverse.
   \[ \Rightarrow \{\mathbb{Z}_4 \setminus \{0\}, \times\} \text{ is not an abelian group.} \]

b) \( GF(2^2) = \{0, 1, x, x+1\} \), where we use \( x^2 + x + 1 \) as irreducible polynomial.

c) \( GF(3^2) = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\} \) with \( h(x)=x^2 +1 \) as irreducible polynomial.
Sol. (con.)

c) Multiplicative inverse of each nonzero element:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(x, x(^{-1}))</td>
<td></td>
</tr>
<tr>
<td>(1, 1)</td>
<td></td>
</tr>
<tr>
<td>(2, 2)</td>
<td></td>
</tr>
<tr>
<td>(x, 2x)</td>
<td></td>
</tr>
<tr>
<td>(x+1, x+2)</td>
<td></td>
</tr>
<tr>
<td>(2x+1, 2x+1)</td>
<td></td>
</tr>
</tbody>
</table>