Written Homework 02

Assigned: Wed 23 Sept 2015  
Due: Wed 7 Oct 2015

Instructions:

• The assignment has to be uploaded to blackboard by the due date. NO assignment will be accepted after 11:59pm on that day.

• We expect that you will study with friends and often work out problem solutions together, but you must write up your own solutions, in your own words. Cheating will not be tolerated. Professors, TAs, and peer tutors will be available to answer questions but will not do your homework for you. One of our course goals is to teach you how to think on your own.

• We require that all homework submissions be neat, organized, and typeset. You may use plain text or a word processor like Microsoft Word or LaTeX for your submissions. If you need to draw any diagrams, however, you may draw them with your hand.

• To get full credit, show intermediate steps leading to your answers, throughout.

Problem 1 [21 pts (3,4,4,6,4)]: MOD, GCD & LCM Computations.

i. Find without calculator

\[ 319 \times 117 \mod 10 \quad 1936 + 2378 \mod 10 \quad 113^{4} \mod 10 \]

ii. Use Euclid’s Algorithm to find GCD(59500, 323).

iii. Using alternating calculations of \((\mod 11)\) and squaring calculate \(38^{22} \mod 11\) (see textbook page 62).

iv. Use the extended Euclid’s algorithm to find an integer solution to

\[ 21x + 17y = 1 \]

v. Find LCM(355, 210) by finding first the GCD(355,210).

Problem 2 [18 pts (4,4,6,4)]: Linear Ciphers.

During an ocean floor exploration expedition, 400 miles east off Florida coast, your ship discovers a wreck of a Spanish galeon. The expedition’s divers bring back to the surface a locked chest which they found in one of the galeon’s compartments. When the chest is carefully unlocked, it turns out to contain just a single sheet of old paper with an indecipherable message
Since none of the crew has any idea what to make of the message, they turn to you, the onboard computer scientist, for help in deciphering the message. Carefully examining the paper under ultraviolet light, you notice a pair of barely visible numbers in the upper right corner of the document: 21, 11.

Suspecting a linear cipher $m \rightarrow 21 \times m + 11 \pmod{26}$ which leaves spaces, commas and periods unchanged you guess the following encoding table.

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>h</th>
<th>i</th>
<th>j</th>
<th>k</th>
<th>l</th>
<th>m</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>n</td>
<td>o</td>
<td>p</td>
<td>q</td>
<td>r</td>
<td>s</td>
<td>t</td>
<td>u</td>
<td>v</td>
<td>w</td>
<td>x</td>
<td>y</td>
<td>z</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>

i. Using the above table encode the message (the ciphertext) into a sequence of integers.

ii. In order to decrypt the ciphertext, you need to subtract 11 from each of the integers and then multiply the result by the multiplicative inverse of 21 (mod 26). Find that inverse.

iii. Using the inverse from ii., decrypt each letter of the galeon’s message.

iv. Decode the message and use Google Translate to find its English translation (on historical grounds, you’re almost certain that the message is in Spanish).

**Problem 3** [14 pts (4,4,4,2)]: Modular Arithmetic.

Arrange the non-zero residues mod 7 (i.e. numbers $\{1, 2, 3, 4, 5, 6\}$) in the shape of a regular hexagon as shown on the picture below. For every number $a \in \{1, 2, 3, 4, 5, 6\}$ find its multiplicative inverse $b \in \{1, 2, 3, 4, 5, 6\}$ and connect the verices $a, b$ with an edge. You will thus obtain the graph on the left. Note that numbers 1, and 6 ($6 \equiv -1 (\text{mod } 7)$) are inverses of themselves and lead to the two looping edges in the graph. To further elucidate the idea, an example for residues mod 13 is also given. Again, 1 and -1 (mod 13) are the only self-inverses:
i. Create a similar diagram for residues mod 17.

ii. Having the graph from i.,
   a) What is the product (mod 17) of any two numbers connected by an edge?
   b) How many self-inverses are there?
   c) Calculate
      \[16! = 1 \times 2 \times 3 \times \ldots \times 16 \pmod{17}\]

iii. a) Assuming that for the prime number \(p = 113\) the above pattern holds, how would you quickly calculate
    \[112! + 1 \pmod{113}\]
    b) What assumptions alluded to in the statement "the above pattern holds" did you need in order to perform your calculation?

iv. For any prime number \(p\) calculate
    \[(p - 1)! + 1 \pmod{p}\]  (†)

Explain your answer. (Note: before the general solution to (†) was found, it was believed that a conclusive answer could not be given because the solution required knowing a formula for prime numbers. According to an anecdote, however, Carl Friedrich Gauss solved the question in 5 minutes during a walk.)

Problem 4 [24 pts (4,4,4,8,4)]: Modular Arithmetic – Contd.
i. For numbers \( n \) which are not primes some residues mod \( n \) do not have multiplicative inverses. For example, 3 does not have an inverse (mod 15). However, every number \( a \in \{1, ..., n - 1\} \) which is relatively prime with \( n \) has a multiplicative inverse. Find the set \( \Phi(15) \) of residues mod 15 which are relatively prime with 15.

ii. Similar to Problem 1, arrange members of \( \Phi(15) \) into a regular polygon (or in a line) and connect vertices that are inverses of each other. How many self-inverses are there?

iii. The number \( \phi(n) \) of residues mod \( n \) that are relatively prime with \( n \) is given by the formula by Euler

\[
\phi(n) = n \prod_{p \text{ is prime} \& p|n} \left(1 - \frac{1}{p}\right)
\]

(each prime number appears exactly once in the above product even if it divides \( n \) with power \( \geq 2 \)). Calculate \( \phi(15) \) and \( \phi(42) \).

iv. The set \( \Phi(n) \) of residues mod \( n \) which are relatively prime with \( n \) is closed under multiplication mod \( n \). That is

for any \( a, b \in \Phi(n) \), we also have \( ab \) (mod \( n \)) \( \in \Phi(n) \)

In particular, for every \( a \in \Phi(n) \), powers

\[ a, a^2, a^3, a^4, ... \ (\text{mod } n) \]

also belong to \( \Phi(n) \). Since \( \Phi(n) \) is finite, we must have a repetition, i.e. for some \( l > k \geq 1 \) the following implications must hold:

\[
 a^k \equiv a^l \ (\text{mod } n) \implies a^l - a^k \equiv 0 \ (\text{mon } n) \implies n \mid a^l(a^{l-k} - 1)
\]

Since, as a member of \( \Phi(n) \), \( a \) is relatively prime with \( n \), we must have \( n \mid a^{l-k} - 1 \), i.e. \( a^{l-k} \equiv 1 \) (mod \( n \)). In other words, for every \( a \in \Phi(n) \), there is a positive integer \( q > 1 \) such that

\[ a^q \equiv 1 \ (\text{mod } n) \]

Let, \( n = 18 \).

a) Calculate \( \phi(18) \)
b) List all elements of \( \Phi(18) \)
c) Calculate \( 5^6 \) (mod 18), \( 7^6 \) (mod 18) and \( 11^6 \) (mod 18).
d) Based on a), b), c) can you complete fill in the blank in the below statement:

If \( a \) is relatively prime with \( n \), then

\[ a^{\phi(n)} \equiv 1 \ (\text{mod } n) \]

v. Knowing that \( a^q \equiv 1 \) (mod \( n \)), for \( q > 1 \), helps with finding multiplicative inverses mod \( n \) because we can then write \( ab \equiv 1 \) (mod \( n \)), where \( b = a^{q-1} \) is the inverse. Using Euler totient function \( \phi(n) \) find the multiplicative inverses of 13 (mod 18) and 4 (mod 21).
Problem 5 [22 pts (2,4,2,6,6,2)]: RSA Cryptosystem.

Suppose that you’re working for the NSA and you know that the enemy is using an RSA cryptosystem with the following parameters.

1. Encoding:
   Their messages are just two letters long and consist of only the 26 small letters of the alphabet. First, they encode each letter into an integer representing its alphabetical position (the second row), and then they convert that position into a 5 bit binary (the third row).

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>h</th>
<th>i</th>
<th>j</th>
<th>k</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>00000</td>
<td>00001</td>
<td>00010</td>
<td>00011</td>
<td>00100</td>
<td>00101</td>
<td>00110</td>
<td>00111</td>
<td>01000</td>
<td>01001</td>
<td>01010</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>l</th>
<th>m</th>
<th>n</th>
<th>o</th>
<th>p</th>
<th>q</th>
<th>r</th>
<th>s</th>
<th>t</th>
<th>u</th>
<th>v</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>01011</td>
<td>01100</td>
<td>01101</td>
<td>01110</td>
<td>01111</td>
<td>10000</td>
<td>10001</td>
<td>10010</td>
<td>10011</td>
<td>10100</td>
<td>10101</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>w</th>
<th>x</th>
<th>y</th>
<th>z</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
<tr>
<td>10110</td>
<td>10111</td>
<td>11000</td>
<td>11001</td>
</tr>
</tbody>
</table>

   Hence the word "to" would be encoded as 10-bit binary number 10011 01110 = 622.

2. The enemy is confident in the unbreakability of their system and advertise their public key $(e, n) = (11, 1517)$.

   i. Suppose that you wanted to confuse the enemy by sending them the an attack signal $P =$ "go". What would be the number $E$ into which you would need encode the plaintext $P$? Write that number both in binary and decimal notation.

   ii. In order to encrypt $P$, you would need to calculate a) $E^{11} \pmod{1517}$ and then b) convert the result to binary. The thus obtained binary number would be the ciphertext $C$ of the original plaintext which you would send to the enemy. Calculate a) using the method of alternate evaluation of (mod 1517) and squaring described in the textbook on page 62. What is the ciphertext $C$?

Decrypting Enemy’s Message

You are told by the human intelligence services that it is of utmost importance to break the enemy’s code in order to decrypt the ciphertext $C = "1100111" = 103$ which was intercepted on its way to the enemy. Break the enemy’s code in the following steps:

   iii. Factor 1517 into a product of two prime numbers $p, q$

   iv. Calculate multiplicative inverse $d$ of 11 mod $(p-1)(q-1)$ using the extended Euclidean Algorithm.
v. Decrypt the ciphertext by calculating $103^d \pmod{1517}$.

vi. Convert the result of part v into binary then and decode the message.

Note: The strength of the RSA system hinges on the difficulty of performing part a) for products of large primes.