Euclid’s Algorithm and the RSA Encryption Scheme

1. For each pair of integers \((a, b)\) below, find \(d = \gcd(a, b)\) and find a pair of numbers \(j\) and \(k\) such that \(d = j \cdot a + k \cdot b\). (Use the Extended Euclidean algorithm.)

   (a) 90 and 56
   (b) 91 and 89
   (c) 711 and 75
   (d) 815 and 75
   (e) 112 and 196
   (f) 366 and 150

2. For each triple of integers \(p, q, e\) given below, find the (smallest positive) value of \(d\) that will work for the private key of the RSA algorithm (where, as usual, \(n = p \cdot q\) and \(\phi(n) = (p - 1)(q - 1)\), and \(ed \equiv 1 \pmod{\phi(n)}\)). Then suppose that the message (integer) \(M = 25\) is to be encoded using the public key \(n, e\) pair. Find the ciphertext that corresponds to that message \(M\).

   (a) \(p = 7, q = 13, e = 5\)
   (b) \(p = 5, q = 11, e = 3\)
   (c) \(p = 7, q = 17, e = 7\)

3. Finally, suppose that \(p = 5, q = 17,\) and \(e = 13\). First find the private key \(d\) for the RSA method with these parameters. Then decrypt the ciphertext messages, \(C\), below to find the original (plaintext) messages.

   (a) 12
   (b) 9
   (c) 27
   (d) 84

Solution:

1. First let us recall the Extended Euclidean algorithm. The pseudocode for this method is given below:

   \[
   \text{ExtendedEuclidGCD}(a, b)
   \]
   
   Input: Nonnegative integers \(a\) and \(b\) (not both zero).
   
   Output: \(d = \gcd(a, b)\), integers \(j, k\) where \(d = j \cdot a + k \cdot b\).

   1 \textbf{if } b = 0 \textbf{ then}
   2 \quad \text{return } (a, 1, 0)
   3 \quad r \leftarrow a \mod b
   4 \quad \text{Let } q \text{ be the integer such that } a = q \cdot b + r \text{ (that is, } q = \lfloor \frac{a}{b} \rfloor).$
   5 \quad (d, j, k) \leftarrow \text{ExtendedEuclidGCD}(b, r)
   6 \quad \text{return } (d, k, j - kq)
We can use this algorithm for each pair of numbers in Question 1. As this is a recursive procedure, we fill in the table below from left to right for the rows involving \( a, b, q, \) and \( r \), and then we fill it in from right to left for the rows involving \( j \) and \( k \). We will assume that \( a \geq b \) (as will always be the case after the first step of the algorithm, so let’s just assume this is the case).

<table>
<thead>
<tr>
<th></th>
<th>90</th>
<th>56</th>
<th>34</th>
<th>22</th>
<th>12</th>
<th>10</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( b )</td>
<td>56</td>
<td>34</td>
<td>22</td>
<td>12</td>
<td>10</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>( q )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>-</td>
</tr>
<tr>
<td>( r )</td>
<td>34</td>
<td>22</td>
<td>12</td>
<td>10</td>
<td>2</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>( j )</td>
<td>5</td>
<td>-3</td>
<td>2</td>
<td>-1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( k )</td>
<td>-8</td>
<td>5</td>
<td>-3</td>
<td>2</td>
<td>-1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

We’re first established that \( \gcd(90, 56) = 2 \).

Having made the recursive function calls, we’re now able to fill in the values of \( j \) and \( k \) from right to left. The last column (as shown) will always be 1 and 0 (assuming that \( a \) and \( b \) are not both 0, of course). To get the values of \( j \) and \( k \) in a column, we use the values of \( j \) and \( k \) from the previous column (the one to its right, as we’re filling in the table from right to left) and the value of \( q \) that is in the same column that we’re currently filling in.

So the final table looks like this:

<table>
<thead>
<tr>
<th></th>
<th>90</th>
<th>56</th>
<th>34</th>
<th>22</th>
<th>12</th>
<th>10</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( b )</td>
<td>56</td>
<td>34</td>
<td>22</td>
<td>12</td>
<td>10</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>( q )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>-</td>
</tr>
<tr>
<td>( r )</td>
<td>34</td>
<td>22</td>
<td>12</td>
<td>10</td>
<td>2</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>( j )</td>
<td>5</td>
<td>-3</td>
<td>2</td>
<td>-1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( k )</td>
<td>-8</td>
<td>5</td>
<td>-3</td>
<td>2</td>
<td>-1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Thus we have \( \gcd(90, 56) = 2 \) and \( 2 = (5) \cdot 90 + (-8) \cdot 56 \).

You can double check your work at each step, as for each column, using those values of \( a, b, j, \) and \( k \), you should always get a linear combination that equals the GCD. For example, we have

\[
2 = (-1) \cdot 22 + (2) \cdot 10
\]

and also

\[
2 = (2) \cdot 34 + (-3)22.
\]

For the remainder of the pairs, we’ll only give the final table.

<table>
<thead>
<tr>
<th></th>
<th>91</th>
<th>89</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( b )</td>
<td>89</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( q )</td>
<td>1</td>
<td>44</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>( r )</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>( j )</td>
<td>-44</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( k )</td>
<td>45</td>
<td>-44</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Hence, \( \gcd(91, 89) = 1 \) and \( 1 = (-44) \cdot 91 + (45) \cdot 89 \).

(c) 
\[
\begin{array}{c|cccc}
 a & 711 & 75 & 36 & 3 \\
 b & 75 & 36 & 3 & 0 \\
\end{array}
\]
\[
\begin{array}{c|cccc}
 q & 9 & 2 & 12 & - \\
r & 36 & 3 & 0 & - \\
\end{array}
\]
\[
\begin{array}{c|cccc}
 j & -2 & 1 & 0 & 1 \\
k & 19 & -2 & 1 & 0 \\
\end{array}
\]
So \( \gcd(711, 75) = 3 \) and \( 3 = (-2) \cdot 711 + (19) \cdot 75 \).

(d) 
\[
\begin{array}{c|cccc}
 a & 815 & 75 & 65 & 10 \ 5 \\
b & 75 & 65 & 10 & 5 \ 0 \\
\end{array}
\]
\[
\begin{array}{c|cccc}
 q & 10 & 1 & 6 & 2 \\
r & 65 & 10 & 5 & 0 \\
\end{array}
\]
\[
\begin{array}{c|cccc}
 j & 7 & -6 & 1 & 0 \ 1 \\
k & -76 & 7 & -6 & 1 \ 0 \\
\end{array}
\]
Hence \( \gcd(815, 75) = 5 \), and we have \( 5 = (7) \cdot 815 + (-76) \cdot 75 \).

(e) 
\[
\begin{array}{c|cccc}
 a & 196 & 112 & 84 & 1 \\
b & 112 & 84 & 28 & 0 \\
\end{array}
\]
\[
\begin{array}{c|cccc}
 q & 1 & 1 & 3 & - \\
r & 84 & 28 & 0 & - \\
\end{array}
\]
\[
\begin{array}{c|cccc}
 j & -1 & 1 & 0 & 1 \\
k & 2 & -1 & 1 & 0 \\
\end{array}
\]
So we have \( \gcd(196, 112) = 28 \) and \( 28 = (-1) \cdot 196 + (2) \cdot 112 \).

(f) 
\[
\begin{array}{c|cccc}
 a & 366 & 150 & 66 & 18 \ 12 \ 6 \\
b & 150 & 66 & 18 & 12 \ 6 \ 0 \\
\end{array}
\]
\[
\begin{array}{c|cccc}
 q & 2 & 2 & 3 & 1 \ 2 \\
r & 66 & 18 & 12 & 6 \ 0 \\
\end{array}
\]
\[
\begin{array}{c|cccc}
 j & -9 & 4 & -1 & 1 \ 0 \ 1 \\
k & 22 & -9 & 4 & -1 \ 1 \ 0 \\
\end{array}
\]
Finally we see \( \gcd(366, 150) = 6 \) where \( 6 = (-9) \cdot 366 + (22) \cdot 150 \).

2. For these problems to find \( d \), we can again use the Extended Euclidean algorithm. The main idea is that given \( e \) and \( \phi(n) \) (where \( \gcd(e, \phi(n)) = 1 \)), we can first find the integers \( j \) and \( k \) such that \( j \cdot \phi(n) + k \cdot e = 1 \).

Then having found \( j \) and \( k \), we can reduce this equation modulo \( \phi(n) \), so
\[
[j \cdot \phi(n) + k \cdot e] \pmod{\phi(n)} \equiv 1 \pmod{\phi(n)}.
\]
But we have
\[
[j \cdot \phi(n) + k \cdot e] \pmod{\phi(n)} \equiv j \cdot \phi(n) \pmod{\phi(n)} + k \cdot e \pmod{\phi(n)},
\]
and
\[
j \cdot \phi(n) \equiv 0 \pmod{\phi(n)} \text{ as } j \cdot \phi(n) \text{ is divisible by } \phi(n).
\]
Thus we conclude that $k \cdot e \equiv 1 \pmod{\phi(n)}$.

Now if $k > 0$ then we can take $d = k$ for the RSA decryption method. However, if $k < 0$, then we will add a multiple of $\phi(n)$ to $k$ until we obtain a positive number and this will be the value of $d$ that we use. Some examples should help to clear this up.

(a) $p = 7$, $q = 13$, $e = 5$

In this case we have $n = p \cdot q = 91$ and $\phi(91) = (p - 1)(q - 1) = 72$. Then we use the Extended Euclidean algorithm.

\[
\begin{array}{c|cccc}
  a & 72 & 5 & 2 & 1 \\
  b & 14 & 2 & 2 & - \\
  q & 2 & 1 & 0 & - \\
  r & -2 & 1 & 0 & 1 \\
  j & 29 & -2 & 1 & 0 \\
  k & -1 & 0 & 1 \\
\end{array}
\]

So we have $(-2) \cdot 72 + (29) \cdot 5 = 1$ implying that $29 \cdot 5 \equiv 1 \pmod{72}$. In this case we can take $d = 29$.

Then we want to compute $25^5 \mod 91$ to encode the given message. First we find that $25^2 \mod 91 = 625 \mod 91 = 79$. Then $25^4 \mod 91 = 79^2 \mod 91 = 6241 \mod 91 = 53$.

Finally $25^5 \mod 91 = 53 \cdot 25 \mod 91 = 1325 \mod 91 = 51$. So the ciphertext message that corresponds to $M = 25$ is $C = 51$.

(You could check that $51^{29} \mod 91 = 25$ but you’d want to use the “fast exponentiation algorithm” that we talked about in class to do this by hand.)

(b) $p = 5$, $q = 11$, $e = 3$

We do the same as before, with $n = 55$ and $\phi(55) = 40$.

\[
\begin{array}{c|ccc}
  a & 40 & 3 & 1 \\
  b & 3 & 1 & 0 \\
  q & 13 & 3 & - \\
  r & 1 & 0 & - \\
  j & 1 & 0 & 1 \\
  k & -13 & 1 & 0 \\
\end{array}
\]

This time we have that $(1) \cdot 40 + (-13) \cdot 3 = 1$. This means that $(-13) \cdot 3 \equiv 1 \pmod{40}$.

Using what we said earlier, to get our value of $d$, we will add a multiple of 40 to the number $-13$ until we get a positive number. Namely, we take $d = -13 + 40 = 27$.

Note that we still have the true congruence $27 \cdot 3 \equiv 1 \pmod{40}$ since $27 \cdot 3 - 1 = 80$ is a multiple of 40.

To encode the message $M = 25$ we want to find $25^3 \mod 55$. Then $25^2 \mod 55 = 20$, and so $25^3 \mod 55 = 25 \cdot 20 \mod 55 = 5$. 

4
The message \( M = 25 \) is encoded as the ciphertext \( C = 5 \) in this case.

(c) \( p = 7, q = 17, e = 7 \)

The procedure is clear now (I hope!). With \( n = 7 \cdot 17 = 119 \) and \( \phi(119) = 6 \cdot 16 = 96 \), we first find \( d \).

\[
\begin{array}{cccc}
a & 96 & 7 & 5 & 2 & 1 \\
b & 7 & 5 & 2 & 1 & 0 \\
q & 13 & 1 & 2 & 2 & - \\
r & 5 & 2 & 1 & 0 & - \\
j & 3 & -2 & 1 & 0 & 1 \\
k & -41 & 3 & -2 & 1 & 0 \\
\end{array}
\]

So as usual we have \( (3) \cdot 96 + (-41) \cdot 7 = 1 \).

Thus \( (-41) \cdot 7 \equiv 1 \pmod{96} \). So we take \( d = -41 + 96 = 55 \).

The message \( M = 25 \) is encrypted as \( C = 25^7 \mod 119 = 32 \).

3. Here we have \( p = 5, q = 17, e = 13 \). Thus \( n = 5 \cdot 17 = 85 \) and \( \phi(85) = 4 \cdot 16 = 64 \). You know the drill by now to find the decryption key \( d \).

\[
\begin{array}{cccc}
a & 64 & 13 & 12 & 1 \\
b & 13 & 12 & 1 & 0 \\
q & 4 & 1 & 12 & - \\
r & 12 & 1 & 0 & - \\
j & -1 & 1 & 0 & 1 \\
k & 5 & -1 & 1 & 0 \\
\end{array}
\]

So \( (−1) \cdot 64 + (5) \cdot 13 = 1 \) and therefore \( 5 \cdot 13 \equiv 1 \pmod{64} \). In this case we have \( d = 5 \).

Using this decryption key, we can decode the messages that we’re given by finding \( C^d \mod 85 = C^5 \mod 85 \).

(a) \( 12^5 \mod 85 = 37 \).

(b) \( 9^5 \mod 85 = 59 \).

(c) \( 27^5 \mod 85 = 57 \).

(d) \( 84^5 \mod 85 = 84 \).

(\text{So 84 is \textquotedblleft decoded\textquotedblright\ as the number 84, and hence, 84 is also encoded as 84.})

For all of these numbers, we can also check that \( M^{13} \mod 85 = C \). For example, we have \( 37^{13} \mod 85 = 12 \) (a small verification that the RSA scheme works as intended).