8211430110073969
866-508-1157

```
\documentclass[12pt]{article}
\usepackage[utf8]{inputenc}
\usepackage{amsmath}
\usepackage{graphicx}
\title{Math 315 Final}
\author{Colby Blair}
\date{December 11th, 2010}
\begin{document}
 \maketitle

 \section*{Problem 1}
  \subsection*{A.}
  To determine the dimension of the fractal, we refere to the class definition of dimension: \\

  \begin{equation}
   c = s ^ d
  \end{equation}
  \begin{equation}
   d = \frac{log(c)}{log(s)}
  \end{equation}
  where
  \begin{description}
       d = dimension \\
       s = scaling factor \\
       c = copies to achieve replication.\\
  \end{description}

  Continuing from here, we can observe that in order for the fractal to replicate itself, it must
reproduce itself 3 times in the x and y directions. This give us a scaling factor s = 3. We can
also see that in the original fractal, there are equivalent sub-parts around the parameter, but non
in the middle. So we have 8 sub-parts, instead of 3 x 3 = 9. This means c = 8. Using equation
(2) above:
  \begin{equation}
   d = \frac{log(8)}{log(3)}
  \end{equation}
  \begin{equation}
   d \approx 1.8928
  \end{equation}


  \subsection*{B.}
```

```
\subsection*{C.}
Given the publis RSA key parameters: \\

\begin{equation}
 m = 1633, e = 17
\end{equation}

we want to find the encrypted text, C, using the class definition for RSA encryption:
\begin{equation}
 C \equiv P ^ e (mod  m)
\end{equation}

We transfer our plaintext letters 'UI' into their integer equivalents, in the order that they are in the alphabet (i.e. A = 00, B = 01, etc): \\

\begin{equation}
 U = 20, I = 08
\end{equation}
\begin{equation}
 'UI' = 2008
\end{equation}

Using the definitions for C, m, and e above:

\begin{equation}
 C \equiv 2008^{17} (\mod{1633})
\end{equation}

2008 exponent 17 is a big number, a little hard to process. We use Binary Exponentiation to reduce the number, and to process the modulo:
\begin{equation}
 2008^{17} = 2008^{16} + 2008^{1}
\end{equation}
\begin{align}
 2008^{1} \equiv 375 (\mod{1633}) \\
 2008^{2} \equiv 187 (\mod{1633}) \\
 2008^{4} \equiv 187^{2} \equiv 676 (\mod{1633}) \\
 2008^{8} \equiv 676^{2} \equiv 1369 (\mod{1633}) \\
 2008^{16} \equiv 1369^{2} \equiv 1110 (\mod{1633}) \\
\end{align}
\begin{align}
 2008^{17} \equiv (1110 * 375)(\mod{1633})
 \equiv 1468(\mod{1633})
\end{align}

Therefore, C = 1468.
```

\subsection*{D.}
To find the decryption value, we use the class definition for P decryption:

\begin{equation}
 P \equiv C^{d}(\mod{m})
\end{equation}
where
\begin{description}
 C = encrypted code (i.e. 1468 from Problem 1.B above) \\
 m is part of the RSA public key as explained in Problem 1.B above \\
 d is given by the equation:
 \begin{equation}
  de \equiv 1 (\mod{\varphi(m)})
 \end{equation}
\end{description}

For d, we need to know that $ \varphi(m) $ equals the number of factors of m. We now have to find d to find e, and $ \varphi(m) $ to find both. We know from Euler's Totient Function that:
\begin{equation}
 \varphi(m) = (p-1)*(q-1)
\end{equation}
where
\begin{description}
 p and q are prime factors of m
\end{description}

If we use some computer programming, we can quickly find that the prime factors of m = 1633 are
p = 23, q = 71. We can then tell that $ \varphi(m) = 22*70 = 1540$. So:
\begin{equation}
 de \equiv 1 (\mod{1540})
\end{equation}

We then apply the Euclidian Algorithm, substituting in the other part of our RSA public key e = 17:
\begin{align}
 d(17) \equiv 1 (\mod{1540}) \\
 \\
 1540 = 17(90) + 10 \\
 17 = 10(1) + 7 \\
 10 = 7(1) + 3 \\
 7 = 3(2) + 1 \\
 \\

1 = 7 - 3(2) \\
1 = 7 - (10 - 7)(2) \\
1 = 7(3) - 10(2) \\
1 = (17 - 10)(3) - (10)(2) \\
1 = 17(3) - 10(3) - (10)(2) \\
1 = 17(3) - 10(5) \\
1 = 17(3) - (1540 - 17(90))(5) \\
1 = 17(3) - 1540(5) + 17(450) \\
1 = 17(453) - 1540(5) \\
17(453) = 1540(5) + 1 \\
\end{align}

We now have an equation of the form $ de \equiv 1(\mod{1540} $:
\begin{align}
453(17) \equiv 1 (\mod{1540}) \\
d = 453
\end{align}

We can now decode with $ d = 453, m = 1633, and C = 1468 $ for the original decryption alrgorithm:
\begin{align}
P \equiv C^{d}(\mod{m}) \\
P \equiv (1468)^{453})\mod{m}
\end{align}

Use the Euclidian Algorithm:
\begin{align}
1468^{453} = 1468^{256} + 468^{128} + 1468^{64} + 1468^{4} + 1468^{1} \\
\end{align}
\begin{align}
1468^{1} \equiv 1468(\mod{1633}) \\
1468^{2} \equiv 1097(\mod{1633}) \\
1468^{4} \equiv 1097^{2} \equiv 1521(\mod{1633}) \\
1468^{8} \equiv 1521^{2} \equiv 1113(\mod{1633}) \\
1468^{16} \equiv 1113^{2} \equiv 955(\mod{1633}) \\
1468^{32} \equiv 955^{2} \equiv 811(\mod{1633}) \\
1468^{64} \equiv 811^{2} \equiv 1255(\mod{1633}) \\
1468^{128} \equiv 1255^{2} \equiv 813(\mod{1633}) \\
1468^{256} \equiv 813^{2} \equiv 1237(\mod{1633}) \\
\end{align}
\begin{align}
1110^{453} \equiv (1237 * 813 * 1255 * 1521 * 1468)(\mod{1633}) \\
\equiv (1386 * 1511 * 1468)(\mod{1633}) \\
\equiv (740 * 1468)(\mod{1633}) \\
\equiv 375(\mod{1633})
\end{align}

Notice that from Problem1.C that $ P \equiv 375(\mod{1633}) \equiv 2008(\mod{1633}) $, so we essentially have gotten our orginal $ P = 2008 = 'UI' $ back. In practice, if we pick a m greater than our highest character coder, we will avoid the problem like having $ 375 \equiv 2008 $. This is usually the case, because we use ASCII code with a highest value around 256, so a 4 block code would equal a highest value of something like 02560256. m will be a hundred or so digits long, so the problem is solved.

\section*{Problem 2}
\subsection*{A.}
The argument that there is no fundemental order or rule to the universe is not currently a strong one. We can easily see th

\end{document}