RSA Cryptographic Systems
Exercises

Dr Basel Halak

1. Solve the following equations

\[ 51x = 63 \mod 71 \]

This means \( x = \frac{63}{51} \mod 71 \)

To find \( x \) we need first to find the multiplicative of 51 in \( \mathbb{Z}_{71} \), we can do this using the Extended Euclidean Algorithm as follows

\[
\begin{align*}
71 &= 51 + 20 \\
51 &= 2 \times 20 + 11 \\
20 &= 11 + 9 \\
11 &= 9 + 2 \\
9 &= 4 \times 2 + 1 \\
2 &= 1 	imes 2 + 0
\end{align*}
\]

By back substitution using equations on the right, we can find:

\[
\begin{align*}
1 &= 9 \times 42 \\
1 &= 9 - 4(11-9) \\
1 &= 5 \times 49 - 4 \times 11 \\
1 &= 5(20-11) - 4 \times 11 \\
1 &= 5 \times 20 - 9 \times 11 \\
1 &= 5 \times 20 - 9(51-2 \times 20) \\
1 &= 23 \times 20 - 9 \times 51 \\
1 &= 23 \times (71-51) - 9 \times 51 \\
1 &= 23 \times 71 - 32 \times 51
\end{align*}
\]

The last equation can be written in \( \mathbb{Z}_{71} \) as follows:

\[ 1 = -32 \times 51 = 39 \times 51 \]

So the multiplicative inverse of 51 is 39 in \( \mathbb{Z}_{71} \), this means

\[ x = \frac{63}{51} = 63 \times 39 = 2457 = 43 \mod 71 \]
2. Use Euclid’s algorithm to find gcd(987, 610)

\[
\begin{align*}
987 &= 1 \times 610 + 377, \\
610 &= 1 \times 377 + 233, \\
377 &= 1 \times 233 + 144, \\
233 &= 1 \times 144 + 89, \\
144 &= 1 \times 89 + 55, \\
89 &= 1 \times 55 + 34, \\
55 &= 1 \times 34 + 21, \\
34 &= 1 \times 21 + 13, \\
21 &= 1 \times 13 + 8, \\
13 &= 1 \times 8 + 5, \\
8 &= 1 \times 5 + 3, \\
5 &= 1 \times 3 + 2, \\
3 &= 1 \times 2 + 1, \\
2 &= 2 \times 1 + 0.
\end{align*}
\]

Thus: gcd(9987, 610) = 1.

3. Factorize 4028033

\[
\sqrt{4028033} \text{ is slightly less than 2007, so try } i = 2007 \text{ giving } i^2 - n = 4028049 - 4028033 = 16 = 4^2 \text{ and hence } n = 20072 - 4^2 = 2011 \times 2003 \text{ (both factors are primes)}.\]