19. A FIRST LOOK AT CRYPTOGRAPHY

We began class by solving another modular equation:

**Example:** Solve $47x \equiv 120 \pmod{1000}$

**Answer:** (Rachel) Note that 47 is prime and does not divide 1000. Therefore, \( \gcd(47, 1000) = 1 \). Hence, 47 has an inverse modulo 1000. To find the inverse, we need to find a solution to the equation $47x + 1000y = 1$. To do this, we implement the Euclidean algorithm:

\[
\begin{align*}
1000 &= 47(21) + 13 \\
47 &= 13(3) + 8 \\
13 &= 8(1) + 5 \\
8 &= 5(1) + 3 \\
5 &= 3(1) + 2 \\
3 &= 2(1) + 1
\end{align*}
\]

For the back substitution, let $a = 1000$ and $b = 47$:

\[
\begin{align*}
a &= b(21) + 13 \implies 13 = a - 21b \\
b &= (a - 21b)(3) + 8 \implies 8 = 64b - 3a \\
a - 21b &= (64b - 3a)(1) + 5 \implies 5 = 4a - 85b \\
64b - 3a &= (4a - 85b)(1) + 3 \implies 3 = 67 = 149b - 7a \\
4a - 85b &= (149b - 7a)(1) + 2 \implies 2 = 11a - 234b \\
149b - 7a &= (11a - 234b)(1) + 1 \implies 1 = 383b - 18a
\end{align*}
\]

Thus, $47(383) + 1000(-18) = 1$ which implies $(383)(47) \equiv 1 \pmod{1000}$. Hence, $47^{-1} \equiv 383 \pmod{1000}$. Now, multiplying both sides of the original equation, we have

\[(383)(47x) \equiv (383)(120) \pmod{1000},\]

which reduces to

\[x \equiv 960 \pmod{1000}.\]

We also made the following remark:

**Remark:** Suppose \( \gcd(a, m) = 1 \) and $1 \leq b, c \leq m - 1$. Suppose $b$ and $c$ are both inverses of $a$ modulo $m$. Then $b = c$. Hence, there is only one inverse of $a$ modulo $m$ (when we reduce to the remainder modulo $m$).

**Proof:** Since $ab \equiv 1 \pmod{m}$ and $ac \equiv 1 \pmod{m}$, we have

\[
\begin{align*}
b &\equiv 1 \cdot b \pmod{m} \\
&\equiv (ac)b \pmod{m} \\
&\equiv c(ab) \pmod{m} \\
&\equiv c \cdot 1 \pmod{m} \\
&\equiv c \pmod{m}.
\end{align*}
\]

Thus, $b \equiv c \pmod{m}$. Since $b$ and $c$ are between 1 and $m - 1$, we must have $b = c$. \qed
Next, Erica showed that if \( a \) has an inverse modulo \( m \), then \( \gcd(a, m) = 1 \):

**Theorem:** Let \( a \) and \( m \) be integers, with \( m \geq 2 \), and suppose \( a \) has an inverse modulo \( m \). Then \( \gcd(a, m) = 1 \).

**Proof:** (Erica) Let \( d = \gcd(a, m) \). We want to show \( d = 1 \), or equivalently (since \( d > 0 \)), that \( d \mid 1 \). Let \( b \) be an inverse of \( a \) modulo \( m \). Then \( ba \equiv 1 \pmod{m} \). This means that \( m \mid ba - 1 \), so \( my = ba - 1 \) for some integer \( y \). Rewriting this equation, we have \( 1 = ba - my \). Now, \( d \) divides \( a \) and \( m \), so \( d \) divides \( ba \) and \( my \). Thus, \( d \) divides \( ba - my = 1 \). \( \square \)

Next, we began discussion of our first application of modular arithmetic: cryptography. The science of cryptography deals with sending and receiving coded messages. Not only governments, but also financial institutions and businesses need frequently to transfer sensitive information from one user or from one computer to another in such a way that even if a message is intercepted by the wrong party, it cannot be read. The general public also needs secure methods of transmitting information, so that, for example, a credit card purchase made over the Internet does not allow one’s name and credit card number to fall into the hands of an unscrupulous thief.

We use the term cipher to mean a system for encoding and decoding messages. We use the term encryption to denote the process of transforming (“encoding”) a plain text message into a coded message and the term decryption to denote the process of transforming (“decoding”) the coded message back into the original plain text message. All modern ciphers are based on mathematics and many are based on techniques and results from number theory.

Historically, people have not only used ciphers to keep their messages secret, but they also have devised ways to keep people from knowing that a message was even being sent. An example of a very old and very simple cipher, based on number theory and purportedly used by Julius Caesar, is the so-called Caesar Cipher. The idea of the Caesar cipher was to use a simple shift of letters. Replace every letter in the plain text message by the letter three places to the right to get the coded message. To decode the coded message, one needs only replace each letter in the coded message by the letter three places to the left. The correspondence is shown in the table below.

<table>
<thead>
<tr>
<th>Cleartext:</th>
<th>A B C D E F G H I J K L M N O P Q R S T U V W X Y Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ciphertext:</td>
<td>D E F G H I J K L M N O P Q R S T U V W X Y X A B C</td>
</tr>
</tbody>
</table>

For example, the word \( \text{CAB} \) would be encrypted as \( \text{FDE} \). This is obviously not a very sophisticated system and would be relatively easy to crack if the message was longer than a few letters.

When discussing cryptography, one usually translates letters to numbers via the following scheme:

<table>
<thead>
<tr>
<th>Letters:</th>
<th>A B C D E F G H I J K L M N O P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numbers:</td>
<td>00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Letters:</th>
<th>Q R S T U V W X Y Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numbers:</td>
<td>16 17 18 19 20 21 22 23 24 25</td>
</tr>
</tbody>
</table>

Note that if we translate letters to numbers, the Caesar cipher amounts to adding 3 and working modulo 26. For example, to encrypting the letter \( \text{U} \) we add 3 to 20 and get 23, which corresponds to \( \text{X} \). To encrypt \( \text{Y} \), we add 3 to 24 and get 27, which is 1 modulo 26,
corresponding to the letter \( B \). To make this precise, the encryption function \( \epsilon \) for the Caesar cipher is
\[
\epsilon(m) = (m + 3) \mod 26
\]
and the decryption function \( \delta \) for the Caesar cipher is given by
\[
\delta(m) = (m - 3) \mod 26.
\]
Notice that \( \delta \) is the inverse function for \( \epsilon \). In other words, for any message \( m \), we have
\[
\delta(\epsilon(m)) = \delta((m + 3) \mod 26) = ((m + 3) - 3) \mod 26 = m.
\]

In general, a shift cipher is described mathematically by \( \epsilon(x) = (x + b) \mod 26 \) for some chosen integer \( b \). The decryption function is then given by \( \delta(x) = (x - b) \mod 26 \). You can check for yourself that \( \delta(\epsilon(x)) = x \) for any message \( x \).

To facilitate discussions in cryptography, we usually assume there are two individuals — Alice and Bob — who are wanting to communicate privately, without their opponent — Oscar — knowing what they are saying to each other. We assume that Oscar has full access to the encrypted messages, however. Of course, we also assume that Oscar knows how to translate letters into numbers and conversely. Shift ciphers are far from secure for several reasons. First, there are only 26 possible shift ciphers, so if we assume that Oscar knows that Alice and Bob are using a shift cipher, it is very easy for him to figure out which one it is. Second, Oscar has only to correctly guess one letter correspondence (which would reveal the value of \( b \)) to crack the whole code.

We can take a step up in complexity from shift ciphers by considering affine ciphers. The idea here is that the encoding function \( \epsilon \) has two parameters: \( a \) and \( b \). We must choose \( a \) so that \( \gcd(a, 26) = 1 \), but \( b \) can be any integer. Then \( \epsilon(x) = (ax + b) \mod 26 \). Let’s consider an example:

**Example:** Consider the affine cipher described by \( \epsilon(x) = (5x + 11) \mod 26 \). We have, for example, \( \epsilon(4) = (5(4) + 11) \mod 26 = 5 \), so the letter \( E \) is encrypted as \( F \).

**Question:** Suppose you intercept the message \( \text{PDQZPSFA} \) which was encrypted using the affine cipher \( \epsilon(x) = (5x + 11) \mod 26 \). Find the decryption function and use it to decrypt the message.

Let \( \delta \) be the decryption function. Note that \( \delta \) is the inverse function of \( \epsilon \), i.e., the function \( \delta \) such that \( \delta(\epsilon(x)) = x \) for any input \( x \). How do we find \( \delta(x) \)? Actually, it’s the same method you use to find inverse functions of real numbers.

Start with \( y = \epsilon(x) = 5x + 11 \mod 26 \). Now interchange the roles of \( x \) and \( y \): \( x = 5y + 11 \mod 26 \). We want to solve for \( y \) in terms of \( x \). Subtracting 11 from both sides, we have \( 5y \equiv x - 11 \pmod{26} \). To get \( y \) by itself on the left-hand side, we need to “divide” by 5. In the modular world, we do this by multiplying by the inverse of 5 modulo 26. (This is why we require \( \gcd(a, 26) = 1 \) in the definition of affine ciphers.) We quickly calculated the inverse of 5 modulo 26 to be 21. That is, \( 21(5) \equiv 1 \pmod{26} \). Multiplying both sides of our equation by 21, we get \( y \equiv 21(x - 11) \equiv 21x + 3 \pmod{26} \). Thus, \( \delta(x) = 21x + 3 \mod 26 \). Once we have the decryption function, we can quickly decode each letter. E.g., the first letter \( P \) gets translated as the number 15. Then \( \delta(15) = 21(15) + 3 \mod 26 = 6 \), which translates to \( G \).

**Homework:**

(1) Decode the message \( \text{PDQZPSFA} \) using the decryption function \( \delta(x) = 21x + 3 \mod 26 \).