Let us return to our examination of ciphers, and make things more mathematical.

We started with the letters A to Z, and wrote down various rules to encode them. Alternatively we can identify $A = 1, B = 2, \ldots, Z = 26$ and work with numbers instead. As we are only interested in these 26 numbers, we may as well work in $\mathbb{Z}_{26}$ (and so $Z = 26 = 0$).

Recall that the Caesar cipher shifted each letter by a constant number of places t. This corresponds to the function $f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$ taking x to $x + t$. The inverse function takes x to $x - t$, and this corresponds to decryption.

In general we will want to consider more than one letter at a time. Suppose we have a function $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ which has an inverse f^{-1}. How can we use this to encode a message? If $n < 26$ then there are not enough numbers, so we assume that $n \geq 26$.

Let t be the largest integer such that $26^t \leq n$. We can now encode a sequence of elements $a_0, a_1, \ldots, a_t \in \mathbb{Z}_{26}$ uniquely as an element of $\mathbb{Z}_n$ as follows:

$$(a_0, \ldots, a_t) \longmapsto \sum_{i=0}^{t-1} a_i (26)^i.$$

(This is like writing a number in base 10 using the digits $0, 1, \ldots, 9$.)

Example 2.21: Let $n = 20,000$.
Now $26^3 = 18,278 \leq n$ but $26^4 > n$. So $t = 3$ and we can encode a triple of letters via

$$(a_0, a_1, a_2) \longmapsto a_0 + 26a_1 + 26^2 a_2.$$

To encode `cabbage` in $\mathbb{Z}_n$ add Zs to the end of the message to make a multiple of 3.

$$\begin{array}{rcl} \texttt{cab} & \longmapsto & 3 + 26 \times 1 + 26^2 \times 2 = 1381 \\ \texttt{bag} & \longmapsto & 2 + 26 \times 1 + 26^2 \times 7 = 4760 \\ \texttt{ezz} & \longmapsto & 5 + 26 \times 0 + 26^2 \times 0 = 5. \end{array}$$

Now to transmit the message Alice sends the elements of $\mathbb{Z}_n$ encoded via f. In this case she sends $f(1381), f(4760), f(5)$.

Bob receives the message and decodes it using f^{-1}. This gives him the numbers from the original plaintext, but he still needs to convert them into letters. However this is straightforward.

Example 2.21: (Continued.)
To convert 1381 back into a_0, a_1, a_2 Bob calculates

$$1381 \mod 26 = 3 = a_0$$

$$\frac{1381 - 3}{26} \mod 26 = 53 \mod 26 = 1 = a_1$$

$$\frac{53 - 1}{26} \mod 26 = 2 \mod 26 = 2 = a_2.$$

and so 1381 corresponds to $3, 1, 2$, ie `cab`.

In this procedure we split our message into sections of length t and encoded each of these as a single unit. Such a cipher is called a block cipher with blocks of length t.

Our cipher thus boils down to the choice of function f. To be able to decode this we need to know the inverse function f^{-1} exists, and how to calculate it.

We have already seen that for the Caesar cipher the function was

$$f(x) = x + a \mod n.$$

This *always* has an inverse,

$$f^{-1}(x) = x - a \mod n.$$

More generally we have affine ciphers of the form

$$f(x) = ax + b \mod n$$

for some $a, b \in \mathbb{Z}_n$. When does such a function have an inverse?

The inverse (when it exists) is given by

$$f^{-1}(x) = a^{-1}(x - b) \mod n$$

for which we require that a^{-1} exists. By Theorem 2.18 this exists if and only if $(a, n) = 1$.

Thus we have an affine cipher $f(x) = ax + b \mod n$ if and only if $(a, n) = 1$.

Example 2.22: (i) Consider $f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$ given by

$$x \longmapsto 7x + 5 \mod 26.$$

This function has an inverse as $(26, 7) = 1$. Indeed the inverse can be calculated using the extended Euclidean algorithm and Bezout's identity. We have $7^{-1} = 15$, so

$$f^{-1}(x) = 15(x - 5).$$

(ii) Consider $g : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$ given by

$$x \longmapsto 4x + 3 \mod 26.$$

This does not have an inverse as $(4, 26) = 2 \neq 1$. Indeed, $g(0) = 3$ and $g(13) = 4 \times 13 + 3 \mod 26 = 3$, so clearly g does not have an inverse.

3. Euler's ϕ function and the Chinese Remainder Theorem

We saw in the last chapter that a has an inverse modulo n if and only if $(a, n) = 1$. It will be useful to know more about such numbers.

Definition 3.1: Let $\phi(n)$ denote the number of elements $x \in \mathbb{Z}_n$ such that $(x, n) = 1$. This is called the Euler ϕ function.

Example 3.2: (i) If p is prime then $(x, p) = 1$ for all $1 \leq x < p$ so $\phi(p) = p - 1$.
(ii) If $n = 8$ then

$$(1, 8) = (3, 8) = (5, 8) = (7, 8) = 1$$

but $(2, 8) = (6, 8) = 2$ and $(4, 8) = 4$. So $\phi(8) = 4$.

In order to understand this function better it will be useful to introduce

Definition 3.3: A reduced residue system modulo n is a set $a_1, a_2, \ldots, a_{\phi(n)}$ of integers such that
(i) If $i \neq j$ then $a_i \not\equiv a_j \mod n$
(ii) We have $(a_i, n) = 1$ for all i.

Clearly p divides x and n if and only if p divides $x + tn$ and n for $t \in \mathbb{Z}$. Thus if $(a, n) = 1$ then $a \equiv a_i \mod n$ for some i, as each a_i is equivalent to some element of $\mathbb{Z}_n$, and this gives every element of $\mathbb{Z}_n$ coprime to n.

Example 3.4: We know from Example 3.2 that $\phi(8) = 4$. A reduced residue system modulo 8 is

$$\{1, 3, 5, 7\}.$$

Another such system is

$$\{17, -5, 5, 15\}$$

as

$$17 \equiv 1 \quad -5 \equiv 3 \quad 5 \equiv 5 \quad 15 \equiv 7 \mod 8.$$

Lemma 3.5: If $\{a_1, \ldots, a_{\phi(n)}\}$ is a reduced reside system modulo n and $(m, n) = 1$ then

$$\{ma_1, \ldots, ma_{\phi(n)}\}$$

is a reduced residue system modulo n.

Proof: As $(m, n) = 1$ there exists $u \in \mathbb{Z}$ such that

$$mu \equiv 1 \mod n \tag{1}$$

by Theorem 2.18, and as $(a_i, n) = 1$ there exist $v_i \in \mathbb{Z}$ such that

$$a_i v_i \equiv 1 \mod n. \tag{2}$$

Now

$$ma_i u v_i = mua_i v_i \equiv a_i v_i \mod n \equiv 1 \mod n$$

by (1) and (2) and so ma_i is invertible modulo n. Hence by Theorem 2.18 we have $(ma_i, n) = 1$.

Next suppose that $ma_i \equiv ma_j \mod n$. Then

$$uma_i \equiv uma_j \mod n$$

and so by (1) we have $a_i \equiv a_j \mod n$, which by assumption implies that $i = j$.

Thus we have shown that $\{ma_1, \ldots, ma_{\phi(m)}\}$ is a reduced residue system modulo n. □

Example 3.6: We saw in Example 3.4 that $\{1, 3, 5, 7\}$ is a reduced residue system modulo 8. Let $m = 7$ and note that $(7, 8) = 1$. Now

$$\{7 \times 1, 7 \times 3, 7 \times 5, 7 \times 7\} = \{7, 21, 35, 49\}$$

and

$$7 \equiv 7 \quad 21 \equiv 5 \quad 35 \equiv 3 \quad 49 \equiv 1 \mod 8$$

so $\{7, 21, 35, 49\}$ is a reduced residue system modulo 8.

One reason for the important of the Euler ϕ function is

Theorem 3.7: (Euler)
Suppose that $a, n \in \mathbb{N}$ with $(a, n) = 1$. Then

$$a^{\phi(n)} \equiv 1 \mod n.$$

Proof: Let $A = \{a_1, a_2, \ldots, a_{\phi(n)}\}$ be a reduced residue set modulo n. By Lemma 3.5, $B = \{aa_1, aa_2, \ldots, aa_{\phi(n)}\}$ is also a reduced residue set modulo n. Therefore each element in B is equivalent to exactly one element in A modulo n. This implies that

$$\begin{aligned} a_1 a_2 \ldots a_{\phi(n)} &\equiv (aa_1) \ldots (aa_{\phi(n)}) \mod n \\ &\equiv a^{\phi(n)} a_1 \ldots a_{\phi(n)} \mod n. \end{aligned}$$

Multiplying both sides by $a_1^{-1} a_2^{-1} \ldots a_{\phi(n)}^{-1}$ (which exists by Theorem 2.18) we get

$$1 \equiv a^{\phi(n)} \mod n$$

as required. □

Corollary 3.8: (Fermat's Little Theorem)
If p is prime then for all a with $(a, p) = 1$ we have

$$a^{p-1} \equiv 1 \mod p$$

and for all $a \in \mathbb{Z}$ we have

$$a^p \equiv a \mod p.$$

Proof: If $(a, p) = 1$ this follows from Euler's Theorem and the fact that $\phi(p) = p - 1$. If $(a, p) = p$ then $a^p \equiv 0$ and $a \equiv 0 \mod p$. □

Suppose that we wish to solve the simultaneous congruences

$$\begin{aligned} x &\equiv 1 \mod 7 \\ x &\equiv 2 \mod 23 \\ x &\equiv 8 \mod 11. \end{aligned}$$

Is there a solution? And if there is then is it unique? The Chinese Remainder Theorem will answer both these questions — and in proving it we will see how to construct such an x.

We will need a few preliminary results. We write $\prod_{i=1}^{n} x_i$ for $x_1 x_2 \ldots x_n$.

Lemma 3.9: Suppose that $m, n_1, \ldots, n_t \in \mathbb{N}$ are such that $(m, n_i) = 1$ for $1 \leq i \leq t$. Then

$$(m, n_1 \ldots n_t) = 1.$$

Proof: As $(m, n_i) = 1$, Bezout's identity (2.7) implies that there exist $u_i, v_i \in \mathbb{Z}$ for $1 \leq i \leq t$ such that

$$1 = u_i m + v_i n_i.$$

By multiplying the RHS of all the equations together we have

$$1 = \prod_{i=1}^{t} (u_i m + v_i n_i).$$

Expanding the RHS, and collecting together all of the terms involving m, we see that

$$\begin{aligned} 1 &= Um + (\textstyle\prod_{i=1}^{t} v_i) n_1 \ldots n_t \\ &= Um + V n_1 \ldots n_t \end{aligned}$$

for some $U, V \in \mathbb{Z}$, and hence by Corollary 2.8 we have

$$(m, n_1 \ldots n_t) = 1.$$

□

Lemma 3.10: If $a, b \in \mathbb{N}$ with $(a, b) = 1$ and $n \equiv 0 \mod a$ and $n \equiv 0 \mod b$ then

$$n \equiv 0 \mod ab.$$

Proof: By assumption we have $n = n_1 a = n_2 b$ for some $n_1, n_2 \in \mathbb{Z}$. By Bezout's identity (2.7) there exist $u, v \in \mathbb{Z}$ with

$$1 = ua + vb.$$

Therefore

$$\begin{aligned} n &= nua + nvb \\ &= n_2 bua + n_1 avb \\ &= (n_2 u + n_1 v)ab \end{aligned}$$

and so ab is a factor of n as required. □

Theorem 3.11:(Chinese Remainder Theorem)
Suppose that $m_1 \ldots, m_t \in \mathbb{N}$ with $(m_i, m_j) = 1$ for $i \neq j$. Then the equations

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_t \mod m_t \end{aligned}$$

have a unique solution modulo $m_1 \ldots m_t$.

Proof: We first show how to construct a solution. Let $M = \prod_{i=1}^{t} m_i$ and $M_i = M/m_i$ for $1 \leq i \leq t$. By Lemma 3.9 we have

$$(m_i, M_i) = 1$$

for $1 \leq i \leq t$, and hence by Theorem 2.18 we can use the extended Euclidean algorithm to calculate $y_i \in \mathbb{Z}$ such that

$$y_i M_i \equiv 1 \mod m_i. \tag{3}$$

We claim that

$$x = \sum_{i=1}^{t} a_i y_i M_i \mod M$$

satisfies the given equations.

First note that

$$a_i y_i M_i \equiv a_i \mod m_i$$

by (3). If $i \neq j$ then m_i divides M_j and so

$$a_j y_j M_j \equiv 0 \mod m_i.$$

Thus

$$x \equiv a_i y_i M_i + \sum_{j \neq i} a_j y_j Mj \equiv a_i \mod m_i.$$

This holds for $1 \leq i \leq t$, and so x is a solution of the given equations.

Now suppose that y is another solution of the same equations. Then

$$x \equiv y \mod m_i$$

for $1 \leq i \leq t$, and hence

$$x - y \equiv 0 \mod m_i.$$

By repeated applications of Lemmas 3.9 and 3.10 we see that

$$x - y \equiv 0 \mod M$$

which implies that $x \equiv y \mod M$ as required. □

Example 3.12: Solve

$$\begin{aligned} x &\equiv 1 \mod 7 \\ x &\equiv 2 \mod 23 \\ x &\equiv 8 \mod 11. \end{aligned}$$

First note that $(7, 23) = (11, 23) = (7, 11) = 1$ and so we may apply the Chinese Remainder Theorem. Let $m_1 = 7$, $m_2 = 23$, $m_3 = 11$, and $a_1 = 1$, $a_2 = 2$, $a_3 = 8$.

$$M = 7 \times 23 \times 11 = 1771.$$

Also $M_1 = 11 \times 23 = 253$, $M_2 = 7 \times 11 = 77$ and $M_3 = 7 \times 23 = 161$.

We need to solve

$$y_i M_i \equiv 1 \mod m_i$$

for $1 \leq i \leq 3$. When $i = 1$ we have

$$253y_1 \equiv 1 \mod 7 \quad \text{or} \quad y_1 \equiv 1 \mod 7$$

so $y_1 = 1$. When $i = 2$ we have

$$77y_2 \equiv 1 \mod 23 \quad \text{or} \quad 8y_2 \equiv 1 \mod 23$$

so $y_2 = 3$. When $i = 3$ we have

$$161y_3 \equiv 1 \mod 11 \quad \text{or} \quad 7y_3 \equiv 1 \mod 11$$

so $y_3 = 8$. (I solved these equations by inspection, but can also find solutions using the extended Euclidean Algorithm.)

Set

$$\begin{array}{rcllll} x & = & a_1y_1M_1 & +a_2y_2M_2 & +a_3y_3M_3 & \mod M \\ & = & 1 \times 1 \times 253 & +2 \times 3 \times 77 & +8 \times 8 \times 161 & \mod 1771 \\ & = & 253 & +462 & +10,304 & \mod 1771 \\ & = & 11,019 & & & \mod 1771 \\ & = & 393. & & & \end{array}$$

It is easy to check that this is a solution of the given equations.

We can now show how to calculate the Euler ϕ function in general.

Definition 3.13: A function $f : \mathbb{N}\backslash\{0\} \longrightarrow \mathbb{N}\backslash\{0\}$ is multiplicative if

$$f(rs) = f(r)f(s)$$

whenever $(r, s) = 1$.

Lemma 3.14: If $(r, s) = 1$ then $(rs, m) = 1$ if and only if

$$(r, m \mod r) = (s, m \mod s) = 1.$$

Proof: Let

$$\begin{array}{lll} m_1 = m \mod r & \text{i.e. } m = m_1 + a_1 r \\ m_2 = m \mod s & \text{i.e. } m = m_2 + a_2 s \end{array} \qquad (4)$$

for some $a_1, a_2 \in \mathbb{Z}$.

First suppose that $(rs, m) = 1$. By Bezout's identity, there exist $u, v \in \mathbb{Z}$ such that

$$urs + vm = 1.$$

From (4) we see that

$$urs + v(m_1 + a_1 r) = 1$$

or

$$(us + va_1)r + vm_1 = 1$$

and so Corollary 2.8 implies that $(r, m_1) = 1$. A similar calculation shows that $(s, m_2) = 1$.

Now suppose that $(r, m_1) = (s, m_2) = 1$. Bezout's identity implies that there exist $w, x \in \mathbb{Z}$ such that

$$wr + xm_1 = 1.$$

From (4) we deduce that

$$wr + x(m - a_1 r) = 1$$

or

$$(w - xa_1)r + xm = 1$$

and so Corollary 2.8 implies that $(r, m) = 1$. Similarly we see that $(s, m) = 1$. By Lemma 3.9 this implies that $(rs, m) = 1$. □

Theorem 3.15: The Euler ϕ function is multiplicative.

Proof: Let $n = rs$ with $(r, s) = 1$. We must show that $\phi(rs) = \phi(r)\phi(s)$. Suppose that $0 \leq m < n$. By the Chinese Remainder Theorem the congruences

$$\begin{array}{ll} x \equiv m \mod r \\ x \equiv m \mod s \end{array}$$

have a unique solution with $0 \leq x < rs$, which is obviously m itself.

Thus each $0 \leq m < n$ corresponds to a unique pair of numbers: $m \mod r$ and $m \mod s$.

By Lemma 3.14, $(m, n) = 1$ if and only if $(m \mod r, r) = 1$ and $(m \mod s, s) = 1$. Now

$$(m \mod r, r) = 1$$

has $\phi(r)$ solutions and

$$(m \mod s, s) = 1$$

has $\phi(s)$ solutions. Thus the equation $(m, n) = 1$ has $\phi(r)\phi(s)$ solutions, as required. □

Corollary 3.16: (i) If $n = p_1^{a_1} \dots p_t^{a_t}$ where the p_i are distinct primes then

$$\phi(n) = \phi(p_1^{a_1}) \dots \phi(p_t^{a_t}).$$

(ii) If p is prime then

$$\phi(p^a) = p^a - p^{a-1}.$$

Proof: (i) follows from Theorem 3.15.
For (ii), note that $(m, p^a) > 1$ only when p divides m. There are exactly p^{a-1} multiples of p which are at most p^a, and so $(m, p^a) = 1$ for $p^a - p^{a-1}$ choices of m as required. □