The Chinese Remainder Theorem

The Chinese remainder theorem guarantees that any simultaneous congruence equation in coprime moduli has a solution. How does one explicitly find a solution? The idea is to explicitly use the second proof of the Chinese remainder theorem presented in class using linear equations. Here is a worked example with some comments.

Question. Find all integers x such that $x - 1$ is divisible by 101, and such that the remainder when x is divided by 37 is 18.

Solution. The two conditions can be stated equivalently as follows:

$$x \equiv 1 \mod 101, \qquad x \equiv 18 \mod 37.$$

Since $\gcd(101, 37) = 1$, the Chinese remainder theorem guarantees a unique solution modulo $37 \times 101 = 3737$. The general solution to the first equation is clearly $x = 1 + 101y$. Substituting this formula into the second equation we find that

$$1 + 101y \equiv 18 \mod 37.$$

Since $101 = 2 \times 37 + 27$, we simplify this to

$$101y \equiv 17 \mod 37,$$

$$27y \equiv 17 \mod 37.$$

Equivalently, we are required to solve the linear equation

$$27y = 17 + 37z,$$

or $27y - 37z = 17$. The method of solving linear equations uses the Euclidean algorithm. We apply the Euclidean algorithm to 27 and 37.

$$\begin{aligned}
&37 = 1 \times 27 + 10 \\
&27 = 2 \times 10 + 7 \\
&10 = 1 \times 7 + 3 \\
&7 = 2 \times 3 + 1 \\
&3 = 3 \times 1
\end{aligned}$$

Working backwards, we find that

$$\begin{aligned}
&1 = 7 - 2 \times 3 \\
&1 = 7 - 2 \times (10 - 1 \times 7) \\
&1 = 3 \times 7 - 2 \times 10 \\
&1 = 3 \times (27 - 2 \times 10) - 2 \times 10\ . \\
&1 = 3 \times 27 - 8 \times 10 \\
&1 = 3 \times 27 - 8 \times (37 - 1 \times 27) \\
&1 = 11 \times 27 - 8 \times 37
\end{aligned}$$

Thus a solution to $27y - 37z = 1$ is given by $(y, z) = (11, 8)$. A particular solution to $27y - 37z = 17$ can be obtained by multiplication by 17; $(y, z) = (187, 126)$. The general solution is therefore given by $(y, z) = (187 + 37k, 126 + 27k)$. In particular,

$$y = 187 + 37k, \text{ and } x = 1 + 101y = 1 + 101(187 + 37k) = 18888 + 3737 \times k.$$

Since $\gcd(101, 37) = 1$, the general solution is therefore

$$x \equiv 18888 \mod 3737$$

or

$$x \equiv 203 \mod 3737.$$

It is worthwhile checking that our solution actually works. One sees that $203 - 1 = 2 \times 101$, and $203 = 5 \times 37 + 18 \equiv 18 \mod 37$.

It is also possible to solve the equations in the reverse order. In this way, we start with $x = 18 + 37y$ and try to solve the equation

$$37y + 18 \equiv 1 \mod 101.$$

We now apply the Euclidean algorithm to 37 and 101. Note that this involves *larger* numbers than before (37 and 27), thus it is often useful to start with the larger modulus first. We are required to solve

$$37y - 101z = -17.$$

One such solution (obtained using the Euclidean algorithm) is $(y, z) = (-1207, -442)$, or $y = -1207 + 101k$, and

$$x = 18 + 37 \times (-1207 + 101k) = -44641 + 3737 \times k \equiv 203 \mod 3737.$$