6.C. Chinese Remainder Theorem problems

Here are some more examples, first solved by using the integers modulo k ($= \mathbb{Z}_k$) for suitable choices of k, and then more directly.

Problem 1. Find all integers n such that $n = 5p + 2$ and $n = 7q + 5$ where p and q are integers.

$\mathbb{Z}_k$ SOLUTION. We need to find p such that $5p + 2 \equiv 5$ modulo 7, which is equivalent to $5p \equiv 3 \bmod 7$. To proceed, we need to find y such that $5y \equiv 1 \bmod 7$; we can do this easily because $5 \cdot 3 = 14 + 1$. Therefore we have $p \equiv 15p = 3 \cdot 5p \equiv 3 \cdot 3 \equiv 2 \bmod 7$ so that $p = 7z + 2$ for some z and $n = 5(7z + 2) + 2 = 35z + 10 + 2 = 35z + 12$.■

DIRECT SOLUTION. We need to find y so that $5y = 1 + 7w$ for some w. As before we can take $y = 3$ and $w = 2$. Then we have

$$3n \;=\; 15p \;+\; 6 \;=\; 21q + 15\ , \quad \text{so that} \quad p \;+\; 6 \;=\; 1 + 7 \cdot (2 + 3q - 2p)$$

so that $p + 5$ is divisible by 7 or equivalently p has the form $7r + 2$ for some r. Thus as in the preceding discussion we have $n = 5(7z + 2) + 2 = 35z + 10 + 2 = 35z + 12$.■

Problem 2. Find all integers n such that $0 < n < 200$ and n can be written as $n = 11p + 6$ and $n = 17q + 8$ where p and q are integers.

$\mathbb{Z}_k$ SOLUTION. We need to find p such that $11p + 6 \equiv 8$ modulo 17, which is equivalent to $11p \equiv 2 \bmod 17$. To proceed, we need to find y such that $11y \equiv 1 \bmod 17$; we can do this easily because $11 \cdot -3 = -34 + 1 = (-2) \cdot 17 + 1$. Multiplying the congruence on the first line by -3, we find that

$$p \;\equiv\; -33p \;\equiv\; (-3) \cdot 11p \;\equiv\; (-3) \cdot 2 \;\equiv\; -6$$

mod 17, so that $p = 17w + 11$ for some w. Substituting in this value, we obtain

$$n \;=\; 11(17w + 11) \;+\; 6 \;=\; 187w \;+\; 121 \;+\; 6 \;=\; 187w \;+\; 127\ .$$

By construction $n \equiv 6 \bmod 11$ and the other congruence follows because $127 = (9 \cdot 17) + 8$. Since $187w + 127$ is not between 0 and 200 if $w \neq 0$, it follows that $n = 127$ is the only solution.■

DIRECT SOLUTION. We need to find y so that $11y = 1 + 17w$ for some w. As before we can take $y = -3$ and $w = -2$. Then we have

$$-3n \;=\; -33p \;-\; 18 \;=\; -51q \;-\; 24\ , \quad \text{so that} \quad p \;=\; -6 + 17 \cdot (2p - 3q)$$

so that $p + 6$ is divisible by 17 or equivalently p has the form $17r + 11$ for some r. Thus as in the preceding discussion we have

$$n \;=\; 11(17r + 11) \;+\; 6 \;=\; 187r \;+\; 121 \;+\; 6 \;=\; 187r \;+\; 127$$

and as before the only solution between 0 and 200 is 127.■

The general procedure

For the sake of completeness, we shall describe the general procedure using the finite number systems $\mathbb{Z}_k$.

The objective is to solve the simultaneous congruences

$$x \equiv c \bmod a \ , \quad x \equiv d \bmod b$$

where a and b are relatively prime (positive) integers and c, d are arbitrary integers. The first congruence means that x has the form $ay+c$, so the problem is to find y such that $ay+c \equiv d \bmod b$. Subtracting c from both sides, we see that the latter congruence is equivalent to $ay \equiv d - c \bmod b$.

Since a and b are relatively prime, there exist integers u, w such that $ua + bw = 1$; we can find them using the Euclidean Algorithm as in `chineseremainder.pdf`. In particular, these imply that $ua \equiv 1 \bmod b$, so that we must have

$$y \quad \equiv \quad uay \quad \equiv \quad u(d-c) \quad \bmod \quad b \ .$$

In other words, y must have the form $u(d-c) + bz$ for some integer z, and consequently we must also have

$$x \quad = \quad au(d-c) \ + \ zab \ + \ c$$

for some z. In particular, this tells us that if solutions exist then they must all be congruent to $au(d-c) + c \bmod ab$.

Finally, we need to verify something which may seem obvious; namely, $x = au(d-c)+c$ actually solves the original pair of congruences. Now $x \equiv c \bmod a$ follows directly from the construction, and using $1 = ua + wb$ we see that

$$x \quad = \quad (1 - wb)(d-c) \ + \ c \quad = \quad (-wb)(d-c) \ + \ (d-c) \ + \ c \quad = \quad d \ - \ bw(d-c)$$

which yields $x \equiv d \bmod b$.■