5. An old Chinese theorem

The Chinese mathematical treatize *Sunzi Suanjing*, written during the 3rd to 5th centuries AD, contains the following puzzle.

> *There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?*

The 7th century Indian mathematician and astronomer Brahmagupta posed the following puzzle.

> *An old woman goes to market and a horse steps on her basket and crushes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?*

The first puzzle asks for 'the' integer $x \geq 0$ that simultaneously satisfies the following system of equations.

$$\left.\begin{array}{rcll} x & \equiv & 2 & \mod 3 \\ x & \equiv & 3 & \mod 5 \\ x & \equiv & 2 & \mod 2 \end{array}\right\} \tag{5.1}$$

The second puzzle asks for the smallest integer $x \geq 0$ that simultaneously satisfies the following system of equations.

$$\left.\begin{array}{rcll} x & \equiv & 1 & \mod 2 \\ x & \equiv & 1 & \mod 3 \\ x & \equiv & 1 & \mod 4 \\ x & \equiv & 1 & \mod 5 \\ x & \equiv & 1 & \mod 6 \\ x & \equiv & 0 & \mod 7 \end{array}\right\} \tag{5.2}$$

We'll provide a method for solving these two classical puzzles (and see that the first has many solutions). To avoid giving away the answers, we'll explain the method with respect to a third variant involving different numbers.

5.1 Variant of the classical puzzles

Let us find the smallest integer $x \geq 0$ that simultaneously satisfies the following system of equations.

$$\left.\begin{array}{rcll} x & \equiv & 3 & \mod 13 \\ x & \equiv & 6 & \mod 14 \\ x & \equiv & 9 & \mod 15 \end{array}\right\} \tag{5.3}$$

We construct a solution x by making a sequence of educated attempts. To start, let us set

$$a \equiv 14^{-1} \mod 13 \tag{5.4}$$

$$b \equiv 15^{-1} \mod 13 \tag{5.5}$$

Our first attempt at a solution to (5.3) is:

$$X = 3 \times 14 \times a \times 15 \times b \tag{5.6}$$

Observe that

$$\begin{array}{rcll} X & \equiv & 3 & \mod 13 \\ X & \equiv & 0 & \mod 14 \\ X & \equiv & 0 & \mod 15 \end{array} \tag{5.7}$$

and so our attempt satifies just the first equation.

As a second attempt set

$$c \equiv 13^{-1} \mod 14 \tag{5.8}$$

$$d \equiv 15^{-1} \mod 14 \tag{5.9}$$

and

$$Y = 6 \times 13 \times c \times 15 \times d\ . \tag{5.10}$$

Observe that

$$\begin{array}{rcll} Y & \equiv & 0 & \mod 13 \\ Y & \equiv & 6 & \mod 14 \\ Y & \equiv & 0 & \mod 15 \end{array} \tag{5.11}$$

and so our attempt satifies just the second equation.

As a third attempt set

$$e \equiv 13^{-1} \mod 15 \tag{5.12}$$

$$f \equiv 14^{-1} \mod 15 \tag{5.13}$$

and

$$Z = 9 \times 13 \times e \times 14 \times f\ . \tag{5.14}$$

Observe that

$$\begin{aligned} Z &\equiv 0 \mod 13 \\ Z &\equiv 0 \mod 14 \\ Z &\equiv 6 \mod 15 \end{aligned} \tag{5.15}$$

and so our attempt satifies just the third equation.

Three failed attempts! But all is not lost. It is pretty obvious that the number

$$x = X + Y + Z \tag{5.16}$$

is a solution to the system (5.3). We can use the above formulae for X, Y and Z to find a simultaneous solution

$$x = 4410 + 15210 + 160524 = 180144 \tag{5.17}$$

to the system (5.3). But is this solution the smallest possible?

Note that $13 \times 14 \times 15 \equiv 0$ on a 13-hour clock, as well as on a 14-hour clock, and also on a 15-hour clock. So for each integer k the number

$$x = 180144 - k \times 13 \times 14 \times 15 \tag{5.18}$$

is a solution to (5.3). Moreover, any solution to (5.3) is of this form. It follows that

$$x = 180144 \mod 13 \times 14 \times 15 \tag{5.19}$$

$$= 21804 \tag{5.20}$$

is the smallest positive integer satisfying (5.3).

5.2 Extracting a theorem

Why did the above method work? It worked because the inverses a, b, c, d, e, f all existed. These inverses existed because $gcd(13,14) = 1$, $gcd(13,15) = 1$ and $gcd(14,14) = 1$. So from the above method we can extract the following.

Theorem 5.2.1 — Chinese Remainder Theorem. For any integers r, s, t and any integers ℓ, m, n satisfying $gcd(\ell, m) = gcd(\ell, n) = gcd(m, n) = 1$, the system of equations

$$\begin{aligned} x &\equiv r \mod \ell \\ x &\equiv s \mod m \\ x &\equiv t \mod n \end{aligned}$$

has a solution.

This theorem can be generalized to systems of more than three equations.