

An ancient problem

An old woman goes to market with a basket of eggs.

A horse steps on the basket, crushing all the eggs.

The horseman offers to pay for the eggs.

The woman can't remember how many eggs she had.

But she does remember that when she took them out 13 at a time there were 3 left over, and there were 6 left over when she took them out 14 at a time, and there were 9 left over when she took them out 15 at a time.

What is the least number of eggs she could have had in the basket?

Chinese Remainder Theorem

Find the smallest non-negative integer x such that the following equations hold simultaneously:

$$\left. \begin{array}{l} x \equiv 3 \pmod{13} \\ x \equiv 6 \pmod{14} \\ x \equiv 9 \pmod{15} \end{array} \right\} (*)$$

Soln

$$\text{Let } a \equiv 14^{-1} \pmod{13}$$

$$b \equiv 15^{-1} \pmod{13}$$

A first attempt at solving (*) is

$$x = 3 \cdot 14 \cdot a \cdot 15 \cdot b$$

$$x \equiv 3 \pmod{13}$$

$$x \equiv 0 \pmod{14}$$

$$x \equiv 0 \pmod{15}$$

$$\text{Let } c = 13^{-1} \pmod{14}$$

$$d = 15^{-1} \pmod{14}$$

Let

$$y = 6 \cdot 13 \cdot c \cdot 15 \cdot d$$

Note

$$y \equiv 0 \pmod{13}$$

$$y \equiv 6 \pmod{14}$$

$$y \equiv 0 \pmod{15}$$

Let

$$e = 13^{-1} \pmod{15}$$

$$f = 14^{-1} \pmod{15}$$

Let

$$z = 9 \cdot 13 \cdot e \cdot 14 \cdot f$$

Note

$$z \equiv 0 \pmod{13}$$

$$z \equiv 0 \pmod{14}$$

$$z \equiv 9 \pmod{15}$$

Now take

$$x \equiv x + y + z$$

Note

$$x \equiv x + y + z \equiv 3 + 0 + 0 \equiv 3 \pmod{13}$$

$$x \equiv x + y + z \equiv 0 + 6 + 0 \equiv 6 \pmod{14}$$

$$x \equiv x + y + z \equiv 0 + 0 + 9 \equiv 9 \pmod{15}$$

$$a \equiv 14^{-1} \pmod{13}$$

$$a = 1$$

$$b \equiv 15^{-1} \pmod{13}$$

$$b \equiv 2^{-1} \pmod{13}$$

$$b = 7$$

$$c \equiv 13^{-1} \pmod{14}$$

$$c \equiv -1 \pmod{14}$$

$$\boxed{c \equiv 13}$$

$$d \equiv 15^{-1} \pmod{14}$$

$$\boxed{d = 1}$$

$$e \equiv 13^{-1} \pmod{15}$$

$$\boxed{e = 7}$$

$$f \equiv 14^{-1} \pmod{15}$$

$$\boxed{f = 14}$$

$$X = 3 \cdot 14 \cdot 1 \cdot 15 \cdot 7$$

$$Y = 6 \cdot 13 \cdot 13 \cdot 15 \cdot 1$$

$$Z = 9 \cdot 13 \cdot 7 \cdot 14 \cdot 14$$

$$x = X + Y + Z$$

$$\equiv 2694$$

$$\pmod{13 \cdot 14 \cdot 15}$$

"So" $x = 2694$ is the smallest non-negative integer satisfying the system (*).

The method works because $\gcd(13, 14) = 1$, $\gcd(13, 15) = 1$, $\gcd(14, 15) = 1$!

The method works for any system

$$\left. \begin{array}{l} x \equiv a \pmod{l} \\ x \equiv b \pmod{m} \\ x \equiv c \pmod{n} \end{array} \right\} (*)$$

with $\gcd(m, n) = 1$, $\gcd(l, n) = 1$,
 $\gcd(l, m) = 1$.