

## An ancient problem

A little 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.

She does remember that when she took the eggs 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 that the woman could have had in her basket?

## Chinese Remainder Theorem

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

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

Sol<sup>n</sup>

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

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

A first attempt at solving (\*) is

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

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

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

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

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

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

$$\text{Let } Y = 6 \cdot 13 \cdot c \cdot 15 \cdot d$$

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

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

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

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

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

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

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

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

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

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

This is called the Chinese remainder theorem, and "clearly" extends to systems of more than three equations.

Now combine the three attempts and set

$$x = X + Y + Z$$

Note:

$$x \equiv X + Y + Z \equiv 3 + 0 + 0 \equiv 3 \pmod{13}$$

$$x \equiv X + Y + Z \equiv 0 + 6 + 0 \equiv 6 \pmod{14}$$

$$x \equiv X + Y + Z \equiv 0 + 0 + 9 \equiv 9 \pmod{15}$$

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

$$a = 1$$

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

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

$$b = 7$$

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

$$c = 13$$

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

$$d = 1$$

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

$$e \equiv (-2)^{-1} \pmod{15}$$

$$e = 7$$

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

$$f = 14$$

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

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

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

$$x = X + Y + Z$$

$$= 18044$$

$$\equiv 2694$$

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

(think!)

"So"  $x = 2694$  is the smallest

integer satisfying the simultaneous equations (\*).

$$13^{-1} \equiv \quad \text{mod } 15$$

$$13 \equiv -2 \quad \text{mod } 15$$

$$13^{-1} = (-2)^{-1} \quad \text{mod } 15$$

$$2 \times 7 \equiv 14 \equiv -1 \quad \text{mod } 15$$

$$\underset{\uparrow}{(-2)} \times 7 \equiv 1 \quad \text{mod } 15$$