HW 7: solution sketches

(1) (Brahmagupta) 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?

Let N be the number of eggs. N is a solution to the system

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 1 \pmod 6 \\ x &\equiv 0 \pmod 7 \end{aligned}$$

The first five congruences can be rewritten as

$$\begin{aligned} x-1 &\equiv 0 \pmod 2 \\ x-1 &\equiv 0 \pmod 3 \\ x-1 &\equiv 0 \pmod 4 \\ x-1 &\equiv 0 \pmod 5 \\ x-1 &\equiv 0 \pmod 6 \end{aligned}$$

which expresses exactly that $x-1$ is divisible by each of $2,3,4,5,6$ (equivalently by $\operatorname{lcm}(2,3,4,5,6) = 60$). Hence our system reduces to the equivalent system

$$\begin{aligned} x &\equiv 1 \pmod{60} \\ x &\equiv 0 \pmod 7 \end{aligned}$$

Since $\gcd(60,7) = 1$ and $\operatorname{lcm}(60,7) = 420$, the full solution is

$$x \equiv 1 \cdot [7^{-1}]_{60} \cdot 7 + 0 \cdot [60^{-1}]_7 \cdot 60 \equiv [7^{-1}]_{60} \cdot 7 \pmod{420}.$$

To find $[7^{-1}]_{60}$, we need to solve $7y \equiv 1 \pmod{60}$, or equivalently $7y + 60z = 1$. This instance of Bézout's identity can be solved by the Euclidean algorithm or by inspection to yield $(y,z) = (43,-5)$.

Returning to the main problem,

$$x \equiv [7^{-1}]_{60} \cdot 7 \equiv 43 \cdot 7 = 301 \pmod{420}.$$

Hence 301 is the smallest positive integer that could be the number of eggs.

(2) Given integers a and b, are the following congruences compatible?

$$\begin{aligned} x &\equiv a \pmod b \\ x &\equiv b \pmod a \end{aligned}$$

Yes.

Solution 1. We must argue that $\gcd(a,b) \mid a-b$. For $d = \gcd(a,b)$, write $a = a'd$ and $b = b'd$. Then $\gcd(a,b) = d$ divides $(a'-b')d = a-b$.

Solution 2. It is enough to show that the system of congruences is solvable. For this, we use inspection to observe that $x = a+b$ is a solution to the system.

(3) I am thinking of a number between 1 and 1000. I am willing to tell you the least significant digit of my number in each of the bases $2, 3, \ldots, 10$. Is this enough information to determine the number? (The least significant digit of a number written $a_n a_{n-1} \cdots a_1 a_0$ in base b is a_0.)

Yes. If the number is N, rewrite the least significant digit in base b of $N = a_n a_{n-1} \cdots a_0$ as $a_{0,b}$. That is, indicate the base in the subscript. We are given the information that $x = N$ is a solution to the system

$$\begin{aligned}
x &\equiv a_{0,2} \pmod 2\\
x &\equiv a_{0,3} \pmod 3\\
x &\equiv a_{0,4} \pmod 4\\
x &\equiv a_{0,5} \pmod 5\\
x &\equiv a_{0,6} \pmod 6\\
x &\equiv a_{0,7} \pmod 7\\
x &\equiv a_{0,8} \pmod 8\\
x &\equiv a_{0,9} \pmod 9\\
x &\equiv a_{0,10} \pmod{10}
\end{aligned}$$

This information determines N uniquely up to $\operatorname{lcm}(2,3,4,5,6,7,8,9,10) = 2520$. This means that there cannot be two distinct solutions to this system of congruences which differ by less than 2520. Hence there can be at most one solution between 1 and 1000.