Chinese remainder theorem.

Theorem. A system of k congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

is consistent (i.e., has a solution) iff each pair of congruences is consistent. If $x = x_0$ is one solution to the system, then the full set of solutions is the set of all integers x satisfying $x \equiv x_0 \pmod{\text{lcm}(m_1, \ldots, m_k)}$.

The pair

$$\begin{aligned} x &\equiv a_i \pmod{m_i} \\ x &\equiv a_j \pmod{m_j} \end{aligned}$$

is consistent iff $\gcd(m_i, m_j)$ divides $a_i - a_j$.

Example. Is the following system of congruences solvable? If so, what is the solution?

$$\begin{aligned} x &\equiv 5 \pmod{14} \\ x &\equiv 13 \pmod{18} \end{aligned}$$

Is the pair of congruences consistent? (Does $\gcd(14, 18) = 4$ divide $5 - 13 = 8$? Yes.) Hence the system is solvable.

Solve $14y + 18z = (5 - 13) = -8$. Then take $x = 5 - 14y = 13 + 18z$. It works. (In this case, $(y, z) = (2, -2)$ is a solution to the linear diophantine congruence, so $x = 5 - 14y = 13 + 18z = -23$ is a solution of the system of congruences. This solution is unique modulo $\text{lcm}(14, 18) = 126$, so the full set of solutions is $x \equiv -23 \pmod{126}$.

Practice with congruences.

(1) Solve $12x \equiv 6 \pmod{50}$.
(2) What is the last (=least significant) digit of 7^{100}?
(3) If $a \equiv 7 \pmod{10}$ and $b \equiv 3 \pmod{15}$, then what are the possible values of $a + b \pmod{20}$?
(4) A bakery opens on September 1, 2012. The baker buys flour in 12 pound bags. She uses 29 pounds of flour per day to bake her goods. One day she notices that the day will end with 21 pounds of flour left in the pantry. What could be the date?

Practice with the CRT.

(1) (Sun Zi, 5th century) Suppose we have an unknown number of objects. When counted in threes, 2 are left over, when counted in fives, 3 are left over, and when counted in sevens, 2 are left over. How many objects are there?

(2) (Brahmagupta, 7th century) 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?

(3) Show that for every positive integer n, there are n consecutive positive integers such that none of them is square-free.

(4) Solve the system

$$\begin{aligned} 2x &\equiv 3 \pmod{3^2} \\ 5x &\equiv 7 \pmod{7^2} \\ 11x &\equiv 13 \pmod{13^2} \end{aligned}$$

(5) Show that there is an integer a such that $z^2 \equiv a \pmod{p}$ is solvable for $p = 3, 5, 7, 11$, but is not solvable for $p = 13, 17$.