Set 7

(A) Diophantine equations

(1) Solve the simultaneous congruence $x \equiv 10 \pmod{102}$ and $x \equiv 5 \pmod 7$. Find at least three solutions.

(2) Find all solutions to the simultaneous congruence $x \equiv 2 \pmod 5$ and $x \equiv 3 \pmod 7$. Then do it for $x \equiv 15 \pmod{29}$ and $x \equiv 19 \pmod{45}$.

(3) Find all integers x, y satisfying $33x + 47y = 1$. Are there any positive solutions? Find all integers z, w satisfying $33z + 47w = 3000$. Are there any positive solutions?

(4) (***HW***) Can we solve the simultaneous congruence $x \equiv 1 \pmod 4$ and $x \equiv 0 \pmod 6$?

(5) Find all integers x satisfying $x \equiv 5 \pmod{24}$ and $x \equiv 7 \pmod{20}$.

(6) For which integers a and b can we always solve simultaneous congruences of the form $x \equiv n \pmod a$ and $x \equiv m \pmod b$?

(7) Find an integer c satisfying $c \equiv 1 \pmod{11}$ and $c \equiv -1 \pmod{13}$. What is $c^2 \pmod{143}$? Find all integer solutions to $x^2 \equiv 1 \pmod{143}$.

(8) (The Hundred Fowls Problem[1]) Suppose one rooster is worth 5 coins, one hen is worth 3 coins, and 3 chicks are worth 1 coin. If I bought 100 fowls with 100 coins, how many roosters, hens, and chicks did I buy?

(B) The Chinese Remainder Theorem, and applications to the φ-function

(1) Find all integers x, with $0 \leq x \leq 120$, with the property $x \equiv 5 \mod 7$ and $x \equiv 4 \mod 8$. Can you find all integers?

(2) Is it possible to find integers x with $x \equiv 1 \mod 6$ and $x \equiv 3 \mod 9$? Why or why not?

(3) Find all integers x satisfying $x \equiv 5 \pmod{24}$ and $x \equiv 7 \pmod{20}$. [Hint: we know we must have $x = 24a + 5 = 20b + 7$.]

(4) Show that, for any integers a and b, we can always find a solution x to the congruence $x \equiv a \mod 3$ and $x \equiv b \mod 5$. Compare to problem (2). What is going on?

(5) For what integers a can you solve the simultaneous congruence $x \equiv 5 \mod 9$ and $x \equiv a \mod 15$?

(6) Suppose that $\gcd(n, m) = 1$. Show that, for any integers a and b, we can always find x satisfying the congruences $x \equiv a \mod n$ and $x \equiv b \mod m$. [Hint: if we can solve the cases $(a, b) = (0, 1)$ and $(a, b) = (1, 0)$ then we can do every case. Why?]

(7) Suppose that $\gcd(n, m) = 1$ and that a and b are integers. Show that any two solutions of $x \equiv a \mod n$ and $x \equiv b \mod m$ must differ by a multiple of nm.

(8) Suppose that $\gcd(n, m) = 1$, and let x be an integer with $0 \leq x < nm$. Show that x is a unit in $\mathbb{Z}/mn$ if and only if x is a unit in both $\mathbb{Z}/m$ and $\mathbb{Z}/n$.

(9) Recall that $\varphi(n) = \#(\mathbb{Z}/n)^\times$ is the Euler φ-function. Show that whenever $\gcd(n, m) = 1$ we have $\varphi(nm) = \varphi(n)\varphi(m)$. Is the statement true if $\gcd(n, m) \neq 1$?

(10) (***HW***) Recall that, if p is a prime number, we have $\varphi(p^k) = p^k - p^{k-1}$. Use this, and the previous problem, to find $\varphi(300)$.

(11) Show that if n is an integer with prime factorization $n = p_1^{k_1} \cdots p_s^{k_s}$ then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$

(12) Suppose that the prime factors of n are $3, 5$ and 71. What fraction of the elements of $\mathbb{Z}/n$ are units?

---

[1] From Wikipedia: The Hundred Fowls Problem is a problem first discussed in the fifth century CE Chinese mathematics text Zhang Qiujian suanjing (The Mathematical Classic of Zhang Qiujian), a book of mathematical problems written by Zhang Qiujian.