Chinese Remainder Theorem

Marcio Woitek

Problem 1

Answer: $N = 5 \cdot 7 \cdot 8 \cdot 9 = 2520$

Problem 2

Answer: $(0, 4, 1, 6)$

In this case, $X = 12345$. It's simple to verify that

$$X \bmod 5 = 0, \tag{1}$$
$$X \bmod 7 = 4, \tag{2}$$
$$X \bmod 8 = 1, \tag{3}$$
$$X \bmod 9 = 6. \tag{4}$$

Therefore, the CRT representation of X is $(0, 4, 1, 6)$.

Problem 3

Answer: It is divisible by both 5 and 8, but may be divisible by other prime factors as well.

To be sure, let's derive the congruence relation that this integer must satisfy. In this case, the moduli are $M_1 = 5$, $M_2 = 7$, $M_3 = 8$ and $M_4 = 9$. It's straightforward to compute the corresponding coefficients A_i. They're given by

$$A_1 = 2016, \tag{5}$$
$$A_2 = 1800, \tag{6}$$
$$A_3 = 945, \tag{7}$$
$$A_4 = 280. \tag{8}$$

Then X satisfies

$$X \equiv A_1 R_1 + A_2 R_2 + A_3 R_3 + A_4 R_4 \equiv 2016\, R_1 + 1800\, R_2 + 945\, R_3 + 280\, R_4 \pmod{2520}. \tag{9}$$

Next, we use the CRT representation of X. By substituting the values of R_i into the last formula, we get

$$X \equiv 480 \pmod{2520}. \tag{10}$$

For concreteness, let's assume that $X = 480$. One can easily check the following facts about this number:
- ▷ it is divisible by 5;
- ▷ it is divisible by 8;
- ▷ it is divisible by 40;
- ▷ since it is clearly even, it is also divisible by 2.

These facts allow us to exclude three of the options. The only remaining option must be the correct one.

Problem 4

Answer: $(9, 16, 35)$

This is the only option such that the product of the moduli equals 5040, and the moduli are pair-wise coprime.

Problem 5

Answer: 10

It's straightforward to show that, for these moduli, the congruence relation that X must satisfy can be written as

$$X \equiv 15\, R_1 + 10\, R_2 + 6\, R_3 \pmod{30}, \tag{11}$$

where R_1, R_2 and R_3 are the residues corresponding to the moduli 2, 3 and 5, respectively.

Problem 6

Answer: 4

It's straightforward to show that, for these moduli, the congruence relation that X must satisfy can be written as

$$X \equiv 288\, R_1 + 441\, R_2 + 280\, R_3 \pmod{504}, \tag{12}$$

where R_1, R_2 and R_3 are the residues corresponding to the moduli 7, 8 and 9, respectively. By substituting the values of these residues into the above expression, we obtain

$$X \equiv 4 \pmod{504}. \tag{13}$$

Problem 7

Answer: $(5, 7, 3)$

For these moduli, the CRT representation of 12345 is $(4, 1, 6)$. The integer 82734 is represented by $(1, 6, 6)$. Then the representation of the sum of these numbers is

$$((4 + 1) \bmod 7, (1 + 6) \bmod 8, (6 + 6) \bmod 9) = (5, 7, 3). \tag{14}$$

Problem 8

Answer: $(4, 6, 0)$

For these moduli, the CRT representation of 12345 is $(4, 1, 6)$. The integer 82734 is represented by $(1, 6, 6)$. Then the representation of the product of these numbers is

$$((4 \cdot 1) \bmod 7, (1 \cdot 6) \bmod 8, (6 \cdot 6) \bmod 9) = (4, 6, 0). \tag{15}$$

Problem 9

Answer: $(5, 5, 1)$

For these moduli, the CRT representation of 46189 is $(3, 5, 1)$. It's simple to check that the following is true:
▷ 5 is the multiplicative inverse of 3 modulo 7;
▷ 5 is the multiplicative inverse of 5 modulo 8;
▷ 1 is the multiplicative inverse of 1 modulo 9.
Therefore, the multiplicative inverse of 46189 is represented by $(5, 5, 1)$.

Problem 10

Answer: $(2, 1, 0)$

We already know that, for these moduli, 12345 is represented by $(4, 1, 6)$. Then the representation of its fifth power can be computed as follows:

$$(4^5 \bmod 7, 1^5 \bmod 8, 6^5 \bmod 9) = (2, 1, 0). \tag{16}$$