Discrete Mathematics - CSCE 531 Fall 2017
In-Class Exercises, Day 6 (18 Oct 17)
Congruences

From Section 4.4

1. (Inspired by Problem 27) Use back substitution to find all solutions, if any, to the following system of congruences:

$$x \equiv 0 (\text{mod}\, 4)$$
$$x \equiv 2 (\text{mod}\, 7)$$
$$x \equiv 7 (\text{mod}\, 9).$$

From the first congruence, we know there exists $i \in \mathcal{Z}$ such that

$$x = 4i + 0 = 4i. \quad (1)$$

Error! Bookmark not defined.

Substitution into the second congruence yields $4i = x \equiv 2 \pmod 7$, from which we can conclude $i \equiv i + 7i = 8i = 2 \cdot 4i \equiv 2 \cdot 2 \pmod 7 = 4 \pmod 7$. Therefore, there exists $j \in \mathcal{Z}$ such that

$$i = 7j + 4, \quad (2)$$

Error! Bookmark not defined.

which we then substitute into Equation (1) to obtain $x = 4 \cdot (7j + 4) = 28j + 16$. Now, substitution into the third congruence yields $28j + 16 \equiv 7 \pmod 9$. Since $28 \equiv 1 \pmod 9$ and $7 - 16 = -9 \equiv 0 \pmod 9$ we have $j \equiv 0 \pmod 9$. Therefore, there exists $k \in \mathcal{Z}$ such that $j = 9k$. Substitution into Equation (2) yields $i = 7 \cdot 9k + 4$, and substitution into Equation (1) gives the solution $x = 4 \cdot 7 \cdot 9k + 4 \cdot 4 = 252k + 16$, which can be written $x \equiv 16 \pmod{252}$.

2. (Inspired by Problem 27) Follow the construction given in Rosen's proof of the Chinese Remainder Theorem to find all solutions, if any, to the following system of congruences:

$$x \equiv 0 (\mathrm{mod}\, 4)$$
$$x \equiv 2 (\mathrm{mod}\, 7)$$
$$x \equiv 7 (\mathrm{mod}\, 9).$$

In the notation of Rosen's proof, we have moduli $m_1 = 4$, $m_2 = 7$, and $m_3 = 9$, as well as remainders $a_1 = 0$, $a_2 = 2$, and $a_3 = 7$.

Because the moduli are pairwise relatively prime and greater than 1, we can apply the Chinese Remainder Theorem. Following the construction given in Rosen's proof of that theorem, we have

$$m = m_1 m_2 m_3 = 4 \cdot 7 \cdot 9 = 252$$

$$M_1 = \frac{m}{m_1} = 7 \cdot 9 = 63$$
$$M_2 = \frac{m}{m_2} = 4 \cdot 9 = 36$$
$$M_3 = \frac{m}{m_3} = 4 \cdot 7 = 28$$

$$y_1 = \overline{M_1} \bmod m_1 = \overline{63} \bmod 4 = 3$$
$$y_2 = \overline{M_2} \bmod m_2 = \overline{36} \bmod 7 = 1$$
$$y_3 = \overline{M_3} \bmod m_3 = \overline{28} \bmod 9 = 1$$

$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= 0 \cdot 63 \cdot 3 + 2 \cdot 36 \cdot 1 + 7 \cdot 28 \cdot 1 \\ &= 268 \end{aligned}$$

Finally, the conclusion of the theorem states that

$$x = 268 \equiv 16 (\mathrm{mod}\, 252)$$

is the unique solution.

3. (Inspired by Problem 39)
   a. Use Fermat's little theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, and $5^{2003} \bmod 13$.

To compute $5^{2003} \bmod 7$, we divide 2003 by $7 - 1 = 6$.

$$2003 = 6 \cdot 333 + 5$$

We then use the result to rewrite the original expression in a form to which we can apply Fermat's little theorem.

$$\begin{aligned} &5^{2003} \bmod 7 = (5^6)^{333} \cdot 5^5 \bmod 7 \\ &= 1^{333} \cdot 5^5 \bmod 7 \\ &= 5^5 \bmod 7 \\ &= \{[(5 \cdot 5 \bmod 7) \cdot 5 \bmod 7] \cdot 5 \bmod 7\} \cdot 5 \bmod 7 \\ &= 3 \end{aligned}$$

The process is identical for the other two parts of the exercise.

$$\begin{aligned} &2003 = 10 \cdot 200 + 3 \Rightarrow 5^{2003} \bmod 11 = (5^{10})^{200} \cdot 5^3 \bmod 11 = 4 \\ &2003 = 12 \cdot 166 + 11 \Rightarrow 5^{2003} \bmod 13 = (5^{12})^{166} \cdot 5^{11} \bmod 13 = 8 \end{aligned}$$

   b. Use your result from part (a) and the Chinese remainder theorem to find $5^{2003} \bmod 1001$. *Hint:* $1001 = 7 \cdot 11 \cdot 13$.

Let $x = 5^{2003}$. Then from part (a), $x \equiv 3 (\bmod 7), x \equiv 4 (\bmod 11), x \equiv 8 (\bmod 13)$.

The application of the Chinese remainder theorem proceeds as follows:

$$a_1 = 3, a_2 = 4, a_3 = 8, m_1 = 7, m_2 = 11, m_3 = 13, m = 7 \cdot 11 \cdot 13 = 1001$$

$$M_1 = 11 \cdot 13 = 143, M_2 = 7 \cdot 13 = 91, M_3 = 7 \cdot 11 = 77$$

$$\begin{aligned} y_1 &= \overline{143} (\bmod 7) = \overline{3} (\bmod 7) = 5 \\ y_2 &= \overline{91} (\bmod 11) = \overline{3} (\bmod 11) = 4 \\ y_3 &= \overline{77} (\bmod 13) = \overline{12} (\bmod 13) = 12 \end{aligned}$$

$$x = 3 \cdot 143 \cdot 5 + 4 \cdot 91 \cdot 4 + 8 \cdot 77 \cdot 12 = 10993 \equiv 983 (\bmod 1001)$$

$$\begin{aligned} 1001k + 983 &= 7(143k + 140) + 3 \checkmark \\ 1001k + 983 &= 11(91k + 89) + 4 \checkmark \\ 1001k + 983 &= 13(77k + 75) + 8 \checkmark \end{aligned}$$

Thus, $5^{2003} \bmod 1001 = x \bmod 1001 = 983$.

From Section 4.5

4. (Inspired by Problem 21) The United States Postal Service (USPS) sells money orders identified by an 11-digit number. The first ten digits identify the money order; and the 11th (last) digit is a check digit that satisfies the sum of the first 10 digits:

$$x_{11} = (x_1 + x_2 + \ldots + x_{10}) \bmod 9 .$$

One digit (Q) in each of these identification numbers of a postal money order is smudged. For each problem, can you identify the value of Q uniquely? If so, what is the value of Q?:

a. 493212Q0688
b. 850Q9103858
c. 2Q941007734
d. 66687Q03201

a.

$$4 + 9 + 3 + 2 + 1 + 2 + Q + 0 + 6 + 8 \equiv 8 (\text{mod } 9)$$
$$Q + 35 \equiv 8 (\text{mod } 9)$$
$$Q \in \{0,9\}$$

b.

$$8 + 5 + 0 + \text{Q} + 9 + 1 + 0 + 3 + 8 + 5 \equiv 8 (\text{mod } 9)$$
$$Q + 39 \equiv 8 (\text{mod } 9)$$
$$Q = 5$$

c.

$$2 + \text{Q} + 9 + 4 + 1 + 0 + 0 + 7 + 7 + 3 \equiv 4 (\text{mod } 9)$$
$$Q + 33 \equiv 4 (\text{mod } 9)$$
$$Q = 7$$

d.

$$6 + 6 + 6 + 8 + 7 + \text{Q} + 0 + 3 + 2 + 0 \equiv 1 (\text{mod } 9)$$
$$Q + 38 \equiv 1 (\text{mod } 9)$$
$$Q = 8$$