Math 328K. Fall 2025

Some solutions to Homework # 7

Prof. Hector E. Lomeli

Section 4.3. Exercise 4. **a)** $x \equiv 37 \pmod{187}$.

b) $x \equiv 23 \pmod{30}$.

c) $x \equiv 6 \pmod{210}$.

d) $x \equiv 150999 \pmod{554268}$.

Section 4.3. Exercise 10. We will solve the system

$$x \equiv 9 \pmod{10}, \qquad x \equiv 9 \pmod{11}, \qquad x \equiv 0 \pmod{13}.$$

The first two equations are equivalent to the single equation $x \equiv 9 \pmod{110}$. Hence, x is of the form $x = 110t + 9$. Substituting in the last equation we find that

$$x \equiv 110t + 9 \equiv 0 \pmod{13}.$$

Given that $110 \equiv 6 \pmod{13}$, we can simplify the equation and get $6t \equiv -9 \pmod{13}$. This implies that $2t \equiv -3 \pmod{13}$. Solving, we find that $t \equiv 5 \pmod{13}$. All solutions are of the form $t = 13u + 5$ and hence all solutions for x are of the form $x = 1430u + 559$. In conclusion, the general solution satisfies $x \equiv 559 \pmod{1430}$.

Section 4.3. Exercise 12. We will solve the system

$$x \equiv 1 \pmod{2}, \quad x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{4}, \quad x \equiv 4 \pmod{5}, \quad x \equiv 5 \pmod{6}, \quad x \equiv 0 \pmod{7}.$$

We will reduce some equations first. We notice that the second, third and fourth equations are equivalent to the system

$$x \equiv -1 \pmod{3}, \qquad x \equiv -1 \pmod{4}, \qquad x \equiv -1 \pmod{5}.$$

By the CRT, these are equivalent to the single equation $x \equiv -1 \pmod{60}$.

We observe that if $x \equiv -1 \pmod{60}$, then x also satisfies $x \equiv -1 \pmod{2}$ and $x \equiv -1 \pmod{6}$. So, the equations modulo 2 and 6 are redundant. To finish the problem, we need to find solutions that also satisfy $x \equiv 0 \pmod{7}$. We get that all solutions are of the form $x = 60t - 1$, so after substitution we find that $4t - 1 \equiv 0 \pmod{7}$. Solving we find that $t \equiv 2 \pmod{7}$. We conclude that the general solution is $x = 60(7n + 2) - 1 = 420n + 119$, where $n \in \mathbb{Z}$. We can also write this as

$$x \equiv 119 \pmod{420}.$$

4. a). Clearly, $(p, q) = 1$. This implies that the CRT can be used to solve the system of equations.

4. c). It is enough to notice that each one of the numbers $\{1, -1, x_0, -x_0\}$ satisfies

$$x \equiv \pm 1 \pmod{p}, \quad x \equiv \pm 1 \pmod{q}.$$

This implies that each number satisfies

$$x^2 \equiv 1 \pmod{p}, \quad x^2 \equiv 1 \pmod{q}.$$

Using the CRT, each element is a solution of $x^2 \equiv 1 \pmod{n}$.

5. We notice that $1417 = 13 \cdot 109$, both prime. If $x^2 \equiv 1 \pmod{1417}$, then

$$x^2 \equiv 1 \pmod{13}, \qquad x^2 \equiv 1 \pmod{109}$$

and therefore

$$x \equiv \pm 1 \pmod{13}, \quad x \equiv \pm 1 \pmod{109}.$$

Solving the general problem,

$$x \equiv a_1 \pmod{13}, \quad x \equiv a_2 \pmod{109},$$

we get the solution

$$x \equiv 872a_1 - 871a_2 \pmod{1417}.$$

Solving each possible case, we get four incongruent positive solutions: $x = 1, 326, 1091, 1416$.

6. a). The number 255 can be written as $255 = 3 \cdot 5 \cdot 17$. Each factor is prime. If we assume that

$$x^2 \equiv 4 \pmod{255},$$

then, using the CRT, we conclude that

$$x^2 \equiv 4 \pmod{3},$$
$$x^2 \equiv 4 \pmod{5},$$
$$x^2 \equiv 4 \pmod{17}.$$

In each case, if p is prime and $x^2 \equiv 4 \pmod{p}$, then either $p|x+2$ or $p|x-2$. Therefore, $x \equiv \pm 2 \pmod{p}$, for $p = 3, 5, 17$.

6. b). We will find the general solution of systems of equations of the form

$$x \equiv a_1 \pmod{m_1}, \qquad x \equiv a_2 \pmod{m_2}, \qquad x \equiv a_3 \pmod{m_3},$$

where $m_1 = 3$, $m_2 = 5$, $m_3 = 17$, and $a_1, a_2, a_2 = \pm 2$. We let $M = m_1 \cdot m_2 \cdot m_3 = 255$, $M_k = M/m_k$ and $M_k y_k \equiv 1 \pmod{m_k}$. Then the general solution of these systems is $x \equiv x_0 \pmod{M}$, where

$$x_0 = a_1 \cdot (M_1 y_1) + a_2 \cdot (M_2 y_2) + a_3 \cdot (M_3 y_3).$$

We have the following numbers.

k	m_k	M_k	y_k	$M_k y_k$
1	3	85	1	85
2	5	51	1	51
3	17	15	8	120

Using all the possible values of a_1, a_2 and a_3, we get the following solutions.

a_1	a_2	a_3	$x_0 = a_1 \cdot 85 + a_2 \cdot 51 + a_3 \cdot 120$	Smallest congruent positive
2	2	2	512	2
2	2	-2	32	32
2	-2	2	308	53
2	-2	-2	-172	83
-2	2	2	172	172
-2	2	-2	-308	202
-2	-2	2	-32	223
-2	-2	-2	-512	253

We conclude that the eight possible incongruent solutions are: 2, 32, 53, 83, 172, 202, 223, 253.