CS 435: Introduction to Cryptography **Fall 2020**

Homework 6

Professor Somesh Jha **Due:** November 28

- **Problem 1 [20 points].** Let $N = pqr$, where p, q, r are three distinct primes. Let $c \geq 1$ be a positive integer such that $c < \min\{p, q, r\}$. Suppose x is an integer that satisfies the following conditions: $x \equiv c \pmod{p}$, $x \equiv c \pmod{q}$, and $x \equiv c \pmod{r}$. Prove that $x \equiv c \pmod{N}$.

  Solution:

  It follows form the CRT (Chinese Remainder Theorem). Indeed, the latter implies that the system

  $$\begin{cases} x \equiv c \pmod{p} \\ x \equiv c \pmod{q} \\ x \equiv c \pmod{r} \end{cases}$$

  has a unique solution modulo N. Moreover, it is trivial to verify that c is a solution, therefore we can conclude that $x \equiv c \pmod{N}$.

- **Problem 2 [30 points].** 1500 soldiers arrive at a training camp. A few soldiers desert the camp. The drill sergeants divide the remaining soldiers into groups of five and discover that there is one left over. When they divide them into groups of seven, there are three left over. When they divide them into groups of eleven, there are again three left over. Determine the number of deserters.

  Solution:

  Let x be the unknown number of remaining soldiers (total minus the deserters), then we can restate the problem as

  $$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 3 \pmod{11} \end{cases}$$

  with $x < 1500$. Since the integers $5, 7, 11$ are relative prime to each other, we can apply the CRT and find a solution of the above system using the formula

  $$M_1 N_1 + 3M_2 N_2 + 3M_3 N_3$$

  where $M_1 = 77$ and N_1 is the inverse of M_1 in the group $\mathbb{Z}_5^*$ (that is, $N_1 M_1 \equiv 1 \pmod{5}$), $M_2 = 55$ and N_1 is the inverse of M_2 in the group $\mathbb{Z}_7^*$, and $M_3 = 35$ and N_3 is the inverse of M_3 in the group $\mathbb{Z}_{11}^*$. To compute the values of N_1, N_2, N_3 we can use the Euclidean algorithm[1]. The result is $N_1 = 3$, $N_2 = N_3 = 6$. Therefore

  $$77 \cdot 3 + 3 \cdot 55 \cdot 6 + 3 \cdot 35 \cdot 6 = 1851$$

[1] If $\gcd(x, y) = 1$, then the Euclidean algorithm outputs a and b such that $ax + by = 1$. This implies that $ax \equiv 1 \pmod{y}$, that is $a \mod y$ is the inverse of x in $\mathbb{Z}_y^*$.

Now, we know that $x \equiv 1851 \pmod{385}$ and that $x < 1500$, therefore we can guess that $x = 1466$. In conclusion, there were 34 deserters.

- **Problem 3 [30 points].** Suppose the $x \equiv 3 \pmod 7$, $x \equiv 3 \pmod{10}$, and $x \equiv 3 \pmod{25}$. Explain why the Chinese Remainder Theorem does not apply to compute x. Transform the problem to an equivalent problem where the Chinese Remainder Theorem can be used and solve it.

  Solution:

  The CRT does not apply to the given system

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 3 \pmod{10} \\ x \equiv 3 \pmod{25} \end{cases} \tag{1}$$

  because $\gcd(10, 25) = 5 \neq 1$ (that is, 10 and 25 are not relatively prime).

  On the other hand, the CRT implies that the congruence $x \equiv 3 \pmod{10}$ is equivalent to the system

$$\begin{cases} x \equiv 3 \pmod 2 \\ x \equiv 3 \pmod 5 \end{cases}$$

  Therefore, system (1) is equivalent to

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 3 \pmod 2 \\ x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod{25} \end{cases} \tag{2}$$

  Now observe that the forth congruence implies the third one, therefore the latter is redundant and can be eliminated. Notice also that we ca rewrite the second congruence as $x \equiv 1 \pmod 2$. Thus, solving system (2) is equivalent to solve system (3)

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 1 \pmod 2 \\ x \equiv 3 \pmod{25} \end{cases} \tag{3}$$

  which can finally be solved using the CRT. We leave to the reader to check that the solution is $x \equiv 3 \pmod{350}$.

- **Problem 4 [20 points].** Let $N = pq$, where p and q are two large odd primes (i.e. think p and q are 1000 bits). Prove that if Oscar can find a message m such that $0 < m < N$ and $m \notin \mathbb{Z}_N^\star$, he can factor N.

  Solution:

  First, recall that $m \notin \mathbb{Z}_N^\star$ means that $\gcd(N, m) \neq 1$. Since $N = pq$ and $0 < m < N$, this implies that $\gcd(N, m) = p$ or $\gcd(N, m) = q$. Without loss of generality, we can assume that $\gcd(N, m) = p$. Then, recall that $\gcd(N, m)$ be efficiently computed via the Euclidean algorithm. In this way, Oscar can compute the prime p and factor N.