

1.

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

Since  $c < \min\{p, q, r\}$ , clearly,  $x=c$  is a solution to the equations above

CRT implies the solutions to the above equations are congruent modulo  $N=pqr$

Therefore  $x \equiv c \pmod{N}$

2.

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

$$M_1 = 77$$

$$M_2 = 55$$

$$M_3 = 35$$

$$N_1 = 3$$

$$N_2 = 6$$

$$N_3 = 6$$

$$77 \times 3 \times 1 + 55 \times 6 \times 3 + 35 \times 6 \times 3 = 1851$$

Since  $x \equiv 1851 \pmod{385}$  and  $x < 1500$

$x = 1466$ . Therefore, there are 34 deserters

3.

The CRT does not apply because  $\gcd(10, 25) = 5 \neq 1$

$$x \equiv 3 \pmod{10} \Rightarrow \begin{cases} x \equiv 3 \pmod{2} \\ x \equiv 3 \pmod{5} \end{cases}$$

$$x \equiv 3 \pmod{25} \Rightarrow x \equiv 3 \pmod{5}$$

$$x \equiv 3 \pmod{2} \Rightarrow x \equiv 1 \pmod{2}$$

The system is equivalent to

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

$$M_1 = 50$$

$$M_2 = 175$$

$$M_3 = 14$$

$$N_1 = 1$$

$$N_2 = 1$$

$$N_3 = 9$$

$$50 \times 1 \times 3 + 175 \times 1 \times 1 + 14 \times 9 \times 3 = 703$$

$$703 \pmod{350} = 3$$

Therefore the solution is  $x \equiv 3 \pmod{350}$

4. If  $m \notin \mathbb{Z}_N^*$ , then  $\gcd(m, N) \neq 1$

Since  $N = pq$  where  $p, q$  are two large primes,  $\gcd(m, N) = p$  or  $\gcd(m, N) = q$

$\gcd(m, N)$  can be computed efficiently using the Euclidean algorithm.

Therefore, Oscar can factor  $N$