

**Problem 7):** We start with values for  $N$  and  $\phi(N)$ . For clarity, we will denote the numerical value for  $\phi(N)$  by the symbol  $\Phi_N$ . Further, we know both that  $N = pq$  and

$$\begin{aligned}\phi(N) &= \phi(p) \phi(q) \\ &= (p-1)(q-1) \\ &= pq - p - q + 1 = \Phi_N\end{aligned}\tag{7.1}$$

Additionally, note that the result in 7.1 was obtained using the relations  $\phi(p) = p-1$  and  $\phi(q) = q-1$ . The result in 7.1, along with  $N = pq$ , means that we have the system of equations

$$\Phi_N = pq - p - q + 1\tag{7.1}$$

and

$$N = pq\tag{7.2}$$

Rewriting the expression in 7.2 as  $N = pq \Rightarrow q = N/p$  and applying the result, along with  $N = pq$  to the expression in 7.1, we have

$$\begin{aligned}\Phi_N &= N - p - \frac{N}{p} + 1 \\ p\Phi_N &= pN - p^2 - N + p \\ 0 &= p^2 + (\Phi_N - N - 1)p + N\end{aligned}\tag{7.3}$$

which is solvable for  $p$  in polynomial time (using the quadratic formula). Applying the result from solving 7.3 for  $p$  to the expression in 7.2 yields a value for  $q$  in polynomial time as well.