

## 4.2 Question 2

**4.2.A** Consider the following hash function. Messages are in the form of a sequence of numbers in  $\mathcal{Z}_n$ ,  $M = (a_1 a_2 \dots a_t)$ . The hash value is calculated as  $\sum_{i=1}^t a_i$  for some predefined value  $n$ . Does this hash function satisfy any of the requirements for a hash function listed in Table 1.

**4.2.B** Repeat part (A) for the hash function  $h = \left( \sum_{i=1}^t (a_i)^2 \right) \bmod n$ .

**4.2.C** Calculate the hash function of part (B) for  $M = (189, 632, 900, 722, 349)$  and  $n = 989$ .

$$\begin{aligned} h &= \left( \sum_{i=1}^5 (a_i)^2 \right) \bmod 989 \\ &= (189^2 + 632^2 + 900^2 + 722^2 + 349^2) \bmod 989 \\ &= (35'721 + 399'424 + 810'000 + 521'284 + 121'801) \bmod 989 \\ &= 1'888'230 \bmod 989 \\ &= 229 \end{aligned}$$