4.2 Question 2

4.2.A Consider the following hash function. Messages are in the form of a sequence of numbers in $\mathcal{Z}_n$, $M = (a_1 a_2 ... a_t)$. 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.

The *Variable Input Size*, *Fixed Output Size*, and *Efficiency* properties are all satisfied. The fourth property, *Preimage Resistant (One-Way Property)*, is not fulfilled as a message only consisting of the value h has the hash-value $H(h) = h$. Also property 5, *Second Preimage Resistant (Weak Collision Resistant)*, is not fulfilled as to any message M the decimal digit 0 can be added to the sequence; leading to the same hash value. Hence, also property 6 is not satisfied.

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

Again the *Variable Input Size*, *Fixed Output Size*, and *Efficiency* properties are all satisfied. Property 4 is also satisfied if n is a large composite number, because taking square roots modulo such an integer n is considered to be infeasible. Properties 5 and 6 are not satisfied as "$-M$" will have the same hash value as M for instance.

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

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

4.3 Question 3

4.3.A State the value of the padding field in SHA-512 if the length of the message is:

5000 bits

1. Calculate size of the data in the last block:

$$5000\ mod\ 1024 = 904$$

2. Add the size of the length field (128 bit) to the last block size:

$$904 + 128 = 1032$$

3. Because 1032 > 1024 the last block is now:

$$1032\ mod\ 1024 = 8$$

4. The length of the padding field is therefore:

$$1024 - 8 = 1016\ bits$$

5. Therefore the padding consists of one 1 and 1015 zeros, hence the value is:

$$\textit{Value of Padding: } 2^{1015}$$

5001 bits

1. Calculate size of the data in the last block:

$$5001 \; mod \; 1024 \; = \; 905$$

2. Add the size of the length field (128 bit) to the last block size:

$$905 + 128 \; = \; 1033$$

3. Because 1032 > 1024 the last block is now:

$$1033 \; mod \; 1024 \; = \; 9$$

4. The length of the padding field is therefore:

$$1024 - 9 \; = \; 1015 \; bits$$

5. Therefore the padding consists of one 1 and 1014 zeros, hence the value is:

$$\textit{Value of Padding: } 2^{1014}$$

5002 bits

1. Calculate size of the data in the last block:

$$5002 \; mod \; 1024 \; = \; 906$$

2. Add the size of the length field (128 bit) to the last block size:

$$906 + 128 \; = \; 1034$$

3. Because 1032 > 1024 the last block is now:

$$1034 \; mod \; 1024 \; = \; 10$$

4. The length of the padding field is therefore:

$$1024 - 10 \; = \; 1014 \; bits$$

5. Therefore the padding consists of one 1 and 1013 zeros, hence the value is:

$$\textit{Value of Padding: } 2^{1013}$$

4.3.B State the value of the length field in SHA-512 if the length of the message is:

5000 bits

0x00000000000000000000000000001388

5001 bits

0x00000000000000000000000000001389

5002 bits

0x0000000000000000000000000000138A

4.4 Question 4

4.4.A Explain the differences in the algorithms of SHA-3 and MD-5. Which one is used today? Why?

Both algorithms add a padding to the message, but MD-5 adds an additional 64 bit length information. SHA-3 splits the message with padding into k parts with each r bits and uses the iteration function f to perform an absorption phase, where each part is padded again, then combined with the previous result into the function. The absorption phase begins with a zero vector initialization. Afterwards the squeezing phase is started from the final result of the absorption phase and in each of the squeezing step a number of r bits are extracted to get the hash value.
MD-5 on the other hand only initializes a 4 word buffer of fixed constants and performs 512 bit steps. SHA-3 is slower than MD-5 due to the higher number of computations performed, this is also the reason why MD-5 is more widely used. It must be mentioned that MD-5 has high security risks, and should not be used for implementations that strive for a high security level. Rather it should only be used for a quick checksum check.