My curiosity to Computer Science was aroused by my favourite anime, which showed me how splendid a video game could be and the progresses in medical field with advanced technologies. Delving deeper into it, CS became increasingly charming, particularly the areas of AI and virtual and augmented reality, offering the possibility to break the limits of the material world and provide players with an immersive game environment.

I attended a CS course for the first time in a summer school at University of Oxford, and since then programming attracted me as it was like communicating with a friend who would give me expected responses, which felt more comfortable than interacting with a human. We had several tasks in the summer school, including designing websites and implementing an encryption and decryption program. Due to my lack of programming knowledge, I had to learn coding from some online materials, from which I gradually developed my self-learning ability and I found that I could learn any other programming language instantly though they have different syntax. To accomplish the encryption program, I searched online for useful functions and came up with several plans. As it was impossible to apply mathematical functions directly to characters, I decided to encode strings into numbers using Unicode, which can be applied to mathematical functions. I used various functions, such as bitwise functions, for characters of different positions in a string to increase the complexity of my encryption and the decryption processes used corresponding inverse functions. After the summer school, I wanted to know more about how to enhance security of encryption. Therefore, I learned XOR and RSA encryptions, mainly about theories and attack approaches. The XOR encryption could be vulnerable if the plaintext has sequences of repeated characters, so keys long enough to cover every bit are used. The RSA algorithm is robust because breaking its key requires large number prime factorisation, an NP-hard problem, which makes it unsolvable by any practical algorithm with a fairly large key. Therefore, its security is guaranteed unless the P=NP question is solved, or a usable quantum computer is invented. Hence, I believe cracking time is one of the keys to improve security and specific maths theorems could be used to decrease the probability of finding the correct key.

As I discovered I was short of knowledge about algorithms, I read a book ‘Aha Algorithm’. I then realised that apart from the feasibility of implementation of an algorithm, the time complexity is also a vital consideration, not only for encryption but all kinds of algorithms. Most algorithms originated from our everyday life rather than profound concepts I used to consider. Basic events and details that we naturally neglect are arranged systematically and turned into well-regulated approaches to address problems efficiently. From the book AIMA, I knew that AI learns from a mass of data and develops the ability to solve problems by itself with stored cases. I believe that AI could compensate for human’s irrational thinking with more rational and efficient strategies.

In 2019, I participated in Euclid Contest and STEP 1 examination (grade 1), harvesting quite good results. While I was preparing, I acquired extra mathematical knowledge beyond A-level syllabus and practiced my logical thinking and problem-solving abilities through connecting parts of questions with correct logic. Also, I found some of this knowledge was related to CS such as number theory, which helped me learn encryption algorithms better. I also attended the BPhO competition, where I honed my self-learning skill through searching resources and practicing by my own.

Gradually knowing more about complicated theories hidden behind seemingly simple computer operations, I felt more excited to expand knowledge about AI and algorithms in university. I have great interest in joining clubs relate to computing and game development and will endeavour to explore more inspiring fields in CS.