Question 1

- How many instance variables are there in Person201? - **3**
- How many constructors are there in Person201? - **2**

Question 2

According to the equals method of the Person201 class, when are two Person201 objects considered to be equal? Is it case sensitive for their names or for the names of their buildings?

Two objects are equal if they have the same class, name, building and floor. It is case sensitive for their names and building names, because it uses the string equals method in both methods.

Question 3

Does the main method of Person201Demo create any objects of type Person201Utilities? If so, why? If not, why is this not necessary?

No. Person201Demo creates an array using a method from Person201Utilities, but this array itself is not an object. The array contains objects of type Person201.

Question 4

Note that your Person201Finder.java program did not need any kind of password to automatically pull data from the people.txt file; it is publicly available on the internet. In one or two paragraphs, reflect on and respond to one or more of the following related questions. This question is graded for honest effort, not correctness.

- Do you think it's a good idea to keep information about individuals publicly available on the internet? What are some pros and cons?
    - **In this case it is not a good idea to keep this information publicly available on the internet. It contains information that could possibly risk the safety of people by sharing their location publicly. Some information about individuals is fine to share publicly, like a business email or other contact information, but things related to whereabouts or identity verification are dangerous to have on the public internet.**
- If you were the designer of a web application that included personal information (such as a social media app), how would you protect the privacy of your users?
    - **End to end encryption is used by many social media platforms such as WhatsApp and Messenger to safeguard people's messages to each other. This greatly reduces the risk of someone with bad intentions reaching your information, since in most cases they would need an encryption key that is stored on your device only. This is the primary way I would protect the information of my users, and it comes at the cost of accessing your users' data.**