Randsino (Crypto)

As in a lot of crypto challenges we get netcat address and the code which runs on the server.
The code is a python script which is using elliptic curve cryptography to generate a pseudo random number. Our task is to 'predict' the next number. Not really knowing too much about elliptic curves, we head to youtube to accumulate some new knowledge about this topic.
We came across two videos from the channel Computerphile (great channel btw).
The first one is about EC in general, the second one is more interesting:

https://www.youtube.com/watch?v=nybVFJVXbww&ab_channel=Computerphile

It talks about a possibility to place a backdoor when generating pseudo random numbers using EC by making the parameter P a multiple of the parameter Q. The video does an amazing job of explaining this subject, so I won't go into detail.

When we look at the script that is provided to us, we see this exact dependence between said parameters.
All that needs to be done now is to implement what was explained in the video. The solver script can be found in the same folder.
Now when we connect to the netcat address, we copy the data into our script (could have been done more elegantly), run it and get our next 'random' number, send it back to the server and all that is left is to enjoy our well deserved flag.