2018/2/11 YanLiang 112889478

1.
The subgroup will be
2->4->8->16->15->13->9->1->2
So the subgroup will be {2*,4*,8*,16*,15*,13*,9*, 1*}
Where a* is defined as a+17Z

2.
From now on as defined in problem 1 I will just write a* as a from convenience.
In (Z/15Z)*={1,2,4,7,8,11,13,14}
Order of ((z/15z)*)=8
Order (1)=1
Since :
2->4->8->1
so:
order (2)=4
Since
4->1
order (4)=2
7->4->13->1
order(7)=4
8->4->2->1
order (8)=4
11->1
order(11)=2
13->4->7->1
order(13)=4
14->1
order(14)=2

3.
When you do
sage:spacea=RDF(log(a,**2**));
sage: spacea
87.43869691476928
So a it self will take 87.44 bits to store it
Then do
sage: spaceb=RDF(log(b,**2**));
sage: spaceb
99.39695627630769
So spaceb=2^100
So if a take space say x in binary then a^2 will take space 2*x in binary

In that way we know that a^b will double the size a taken by 100 times, since b=2^100
So the total GB to store a will be estimately will be this much:
(88/8)(bytes)*2^100/(2^30)=11*(2^70)=12986507827891524337664

4.
So first of all my id number a=112889478 is not a multiple of p =
135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563

Then we try to see if a^(p-1)=1 if this is not 1 then, we know that p is not a prime number

This will be under the ring of z/pz, so every thing should mod p
So we can do that R(a)^(p-1)
sage: R(a)^(p-**1**)
937281815412093951345919359116580166597919005010914652741455633220771427752844088310393756899396271705739549753435146155011462952634783420319544376989777607328018965025738409525936321678477809891576981236687770677794649237875840202142084143564502741810075801105052147421758408427675192938443840475262808411196
And that is not 1 , so we know that RA-1024 is not a prime number but a composite number.