Discrete Mathematics: Homework 3

(Deadline: 8:00am, March 11, 2022)

1. (15 points) Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$, and let $q = \lfloor a/b \rfloor$. Show that $\ell(a) - \ell(b) - 1 \leq \ell(q) \leq \ell(a) - \ell(b) + 1$, where $\ell(x)$ is the length of the binary representation of an integer x.

2. (25 points) Implement EEA (Extended Euclidean Algorithm). Run your program on the integers a, b to find two integers s, t such that $\gcd(a, b) = as + bt$, where

   a=16680223846514478258525934578333599539857711346377301265204970111653892397676043794016150507259410995658188057040712085903607220122413595420007489488405731334280061988395608779010713411287131295428179813333359977034173092335579409810742439731878889187445253126904842513990354679981309972227336575079548411574454057133261948502170654953266704862335547650976687291747849350782598464591428327947848142796066981940848596121777048411057049426221708373813396661449882414643261467806037889440842533384968180620271785010057924587366185944297155319798570577070773474129972107871623872384643401132513116574551025071336188925411;

   b=17855770299870519367242059681390424418096182155342041137488796879671107478743572864002383145021454681629377265833889126584206834902794697518171431222912791170447567040871094490052067407306798661337490592199170717969818501521767458577818192499457245780503918087449739410569911194050665897532807959319750868264903299819242751930003066441776015464336357481344549028678389909625259705769654505066857444104947192647667108605714724299029223354866042954807541588937325411249097096068333555976598698947608331063572282201472029299051787515328011628625087966449702534156436266476618723897816432054896528012909122280046552133534.

   (**Remark**: Submit your program. The programming can be done with Python, C or C++.)

3. (25 points) Implement the Square-and-Multiply algorithm. Run your program to compute $a^e \bmod n$, where

   a=26430018304661698227244889550916468317489455778956328592921983469699792309163665193972706206594036869415691968221117606771494540098970766552365207210568611105852640630040412543297842462434526788081852074542946114404279053789976397875435006094029065093695673255562607050336148424707698012085470002233698228862346738763599120210887024055251199687451392437357330469313875769415203278005429487989371958004062135384988676187092753933346466785135069682592239769739616884935612245424974736666329142491909330198993521032748920319427468193197363789859738402941190883470502934385251934875320122360082927644910373611459923294476;

   e=14409405982160132058252555071975393865919464165649477935316970889691161917952 93

```
83384024206261698498692401998173408187858576610409025211779025228656559593159550 2
72963336585756256791716496482374867151078740388480801467604318081600477582678868 1
65631594608812754533049620885987507899476027632315364988036894150082485423069839 9
05858727323030674427604859394835304992067509266236322183377936083054953534777979 3
70552131037225482870892396750299984552378371226654317884869633922823332188973055 3
65819358585348317056169095066146081372653285844964902099766835105394381844186194 2
12304890650339820871669368512930619233634553382336 31;

n=64543139452648583804777033627501791038942806480746416798824757337964931888296 53
94087753253738962962018330194333365917018506041929580090385188292077167850690847 7
67373891270856068614351510879149787895083546210864370980484897831652886630906679 3
09597380705323710624409864024826961679269703713720703782658092777661557350773640 0
13648437866289655346805208172279134358934890394382223195659502850096894648865965 3
13811369974332119608428267479786899340636046827882465499287607551454690517628660 2
29163152343334253334664413363549646650010265235190030327641741247445089987600694 2
53212861843109081094890804742752094309113120556963 78.
```

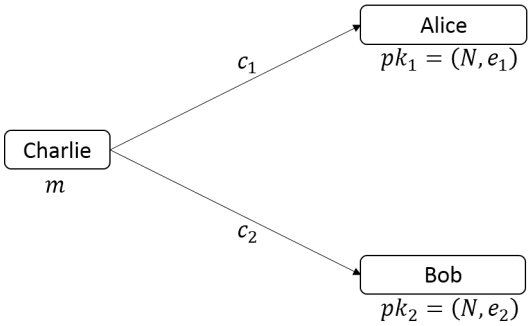
(**Remark**: Submit your program. The programming can be done with Python, C or C++.)

4. (20 points) Solve the following linear congruence equations:

   (1) $17x \equiv 11 (\mathrm{mod} 23)$;

   (2) $55x \equiv 35 (\mathrm{mod} 75)$.

5. (15 points) See the following figure. Alice and Bob trust each other very much. They set their RSA public keys as $pk_1 = (N, e_1)$ and $pk_2 = (N, e_2)$, respectively. Charlie wants to send a private message m to Alice and Bob, where $0 \leq m < N$ is an integer and $\gcd(m, N) = 1$. To this end, Charlie encrypts m as $c_1 = m^{e_1} \bmod N$ and $c_2 = m^{e_2} \bmod N$; and then sends c_1 to Alice and sends c_2 to Bob.



   Suppose that $\gcd(e_1, e_2) = 1$ and Eve sees all public keys and ciphertexts. Determine if Eve can learn the value of m.