Discrete Mathematics: Homework 7

(Deadline: 10:00am, April 24, 2020)

1. (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++.)

2. (25 points) Implement the Square-and-Multiply algorithm. Run your program to compute $a^e \bmod n$, where

   a=26430018304661698227244889550916468317489455778956328592921983469699792309163665193972706206594036869415691968221117606771494540098970766552365207210568611105852640630040412543297842462434526788081852074542946114404279053789976397875435006094029065093695673255562607050336148424707698012085470002233698228862346738763599120210887024055251199687451392437357330469313875769415203278005429487989371958004062135384988676187092753933346466785135069682592239769739616884935612245424974736663291424919093301989935210327489203194274681931973637898597384029411908834705029343852519348753201223600829276449103736114599232944 76;

   e=14409405982160132058252555071975393865919464165649477935316970889691161917952938338402420626169849869240199817340818785857661040902521177902522865655959315955027296333658575625679171649648237486715107874038848080146760431808160047758267886816563159460881275453304962088598750789947602763231536498803689415008248542306983 99;

```
05858727323030674427604859394835304992067509266236322183377936083054953534777979370552131037225482870892396750299984552378371226654317884869633922823332188973055365819358585348317056169095066146081372653285844964902099766835105394381844186194212304890650339820871669368512930619233634553382336315;

n=64543139452648583804777033627501791038942806480746416798824757337964931888296539408775325373896296201833019433336591701850604192958009038518829207716785069084776737389127085606861435151087914978789508354621086437098048489783165288663090667939573807053237106244098640248269616792697037137207037826580927776615573507736400136484378662896553468052081722791343589348903943822231956595028500968946488659653138113699743321196084282674797868993406360468278824654992876075514546905176286602291631523433342533346644133635496466500102652351900303276417412474450899876006942532128618431090810948908047427520943091131205569637 8.
```

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

3. (15 points) Decrypt the ciphertext c in RSA, where

```
p=92848022024833655041372304737256052921065477715975001419347548380734496823522565044177931242947122534563813415992433917108481569319894167972639736788613656007853719476736625612543893748136536594494005487213485785676333621181690463942417781763743640447405597892807333854156631166426238815716390011586838580891;

q=14960085493382551215982833152717710968911855521238517083138736580400843736791361364395996866896561427055911347285154475818328278964312946922654855515046478022953808659049885371810205246851987678819286509222974964354671079346430524381583626702477008188904720017295243800058780798609610767501228426910178511447 1;

e=40998521736306818227223396602297017934844970775490230507394067442991947407942858415658948571832573059620916584782564034578984962597554741990726350973273989719900922249181032503754557074989287122019453704616444256374230446163480285466548201345320125444335191585314853004623900975927763520176673866326616786815005427668354690564900399283808779797121590809053488694752179398441737516982414426626119904064923004119005728475328847480928605634959147345272936348732923564630761782948819009683739182920645278553069258988184216460576162388732542519399531449485509224562557436071560135098226059433823525822521293661707711863337;

c=19650041330069746599953145601677238965601628239920147634666762951565687801813247591184663561168274224394095138658205704008103809773333978958100232545151822422312448751736588990050489889426668766147980463517760613100948096799389143689382182898067907249926601510787188645051967549072611352212571461142898751490154313015692075271086386849897897297470977666504819838227427889585285942150029406458066620610418259125625932693293695504708546297114221671603504978821320540384030274931058558406068460630295717583862204341896109717245183304380824015928953542554305995152146616603959515763932214419921347574243502050051888427885 4.
```

4. (20 points) Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x \star y = xy - x - y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, \star)$ is an Abelian group.

5. (20 points) Let $(G, \cdot)$ be a multiplicative (Abelian) group of order m. Show that $o(a)|m$ for any $a \in G$, i.e., the order of any group element must be a divisor of the group's order.

   (**Hint**: Use the division algorithm.)

6. (15 points) Let $G = \langle g \rangle$ be a subgroup of $\mathbb{Z}_p^*$ of order q, where

   p=17976931348623159077293051907890247336179769789423065727343008115773267580550096313270847732240753602112011387987139335765878976881441662249284743063947412437776789342486548527630221960124609411945308295208500576883815068234246288147391311054082723716335051068458629823994724593847971630483535632962422799885 9,

   $q = (p-1)/2$ and $g = 3$. Suppose that in a Diffie-Hellman key exchange protocol Alice and Bob exchanged the following information $(q, G, g; A, B)$, where

   A=11298357516300261894758966666673542818168451784514487509690291006643472395262301660339321250121412739990882322349247872597126604275489279817778126751282160747054528305947268903473131302761986422868846643825832755204543759020379063550672860377479902112704987257198325450699392115371873979676929609740471744810 8;

   B=11177276780521023949636519169151688104339498819629706201385364667457474340104273644732888615642962919269160152639836608801273674945462668628146757920567508446198949451329462406607413724791303733004048727534691325334573342976778190097710268718537841166014719029641231330332153358610255212345749956378925532136 9.

   In particular, $\log_g A, \log_g B \leq 10^4$. Find the output of Alice and Bob.