cryptohack Mathematics 部分 wp by crumbling

目录

Mathematics

MODULAR MATH

Quadratic Residues

二次剩余

```
p=29
key=[14,6,11]
for j in range(3):
    for i in range(1, p):
        if i ** 2 % p == key[j]:
            print(i,key[j])
```

Legendre Symbol

勒让德符号

```
p =
10152403517453989048540857567108526178875896518906016448438569080146616735666703
66779329988897254765824217387885007387385031343561581972474738502735653492495738
67251280253564698939768700489401960767007716413932851838937641880157263936985954
88165788949758348553552761357845762839917397181054167083854330915913 9
ints =
[25081841204695904475894082974192007718642931811040324543182130088804239047149 28
33347005306004685282989209301502218716662971943950614625927815512751616954111670
49544771049769000895119729307495913024360169904315078028798025169985966732789207
32020386185823404887250863351449838439049704841601292808648032683280 3,
45471765180330439060504647480621449634904192839383897212809808339619841633826534
85610999902796262038187487808699112585424710835969979991377691722705828609042648
45483493881389355042996092003778990527166633511886640963026727120785086013117258
63678223874157861163196340391008634419348573975841578359355931590555,
17364140182001694956465593533200623738590196990236340894554145562517924989208719
24542955764525495352765804924673758953828033201053302706247768423793322119863994
89387842445104691388268081873656783225479920997152292186154759237548969603631388
90331502811292427146595752813297603265829581292183917027983351121325,
14388109104985808487337749876058284426747816961971581447380608277949200244660381
57056853112977505368425607181983729443606913359277254358273598585550625066093857
42349587542113492152932816452053540699707901552370334360654345720206529556668557
73232074749487007626050323967496732359278657193580493324467258802863,
43794993083107728210040904476507850953566435904117063581192391666620894286855627
19233435615196994728767593223519226235062647670077854687031681041462632566890129
59550643018860223875345033769144129304271690990169257097195507892469930687319198
39535010933434232484829606430559434130317685217826346795362762333 18,
85256449776780591202928235662805033201684571648990042997557084658000067050672130
15273491191958166152395707599276166231526268503011525593835254003229711361568781
59760393905377167078545699805166902465921129367969175040347114184654428933234394
90171095447109457355598873230115172636184525449905022174536414781771,
50576597458517451578431293746926099486388286246142012476814190030935689430726042
81045834482856391300101241570287619970821687502099711208969375963845490009258074
66386310621179618766115458511576138357246350052537923161423792390476543929704153
43694657580353333217547079551304961116837545648785312490665576832987,
96868738830341112368094632337476840272563704408573054404213766500407517251810212
49451586217635691691262717228044614120266164019123733656873106932790610089617877
62453116898579970121875991408759120265896726299352678446969769808903807308675200
71059572350667913710344648377601017758188404474812654737363275994871,
48812616568466388006235496629433932343610618271286101200463156497070782441803136
61063004390750821317096754282796876479695558644108492317407662131441224257537276
27496237202127358347850941635876470609847184953603618492464059388890285944138847
28568225414520411812443371247676661616458271454087819176584235717 21,
18237936726367556664171427575475596460727369368246286138804284742124256700367133
25007860853712987796828788545741795786858055337199941422748473760368899262095320
01436880610240926235564710530064641232051338946079238013719860274582743437378603
95496260538663183193877539815179246700525865152165600985105257601565]
for i in range(10):
    if pow(ints[i],(p-1)//2,p):
        d = (p + 1) // 4
        x = pow(ints[i], d, p)
        print(x)
```

Modular Square Root

二次同余方程

当时的代码好像是偷来的脚本，后来有遇见过同样的问题但是一时间没找到，这里先贴个sage的求解吧。

```
p=30531851861994333252675935111487950694414332763909083514133769861350960895076504687261369815735742549428789138300843082086550059082835141454526618160634109969195486322015775943030060449557090064811940139431735209185996454739163555910726493597222646855506445602953689527405362207926990442391705014604777038685880527537489845359101552442292804398472642356609304810680731556542002301547846635101455995732584071355903010856718680732337369128498655255277003643669031694516851390505923416710601212618443109844041514942401969629158975457079026906304328749039997262960301209158175920051890620947063936347307238412281568760161
a=84799946583167721519416165100971270875545412748124351120094257785954953597002444704006424037470585668071278141653966402158441923279004541162579794874320167693299707670467350912498986780880616347965595567049598464241318204160484365013876172117701242927933080792141531799776244404386169585750583611939756866200464398773083399892956045378674936838727788439217713073056027763987869783538662316614533760567719720697763989990137695889361948593449412682231841972313688870606092128755075189361720607022095571244304771374218471306826016669686916514472369170186349024077047973285094618548424320150098780113540221086614610247 68
R.<x> = Zmod(p)[]
f=x^2-a
enc=f.roots()
print(min(enc[0][0],enc[1][0]))
```

Chinese Remainder Theorem

中国剩余定理，这东西还是很有用的

当时也是找了python的脚本，同样先贴个sage的吧。

```
n = [5,11,17]
c = [2,3,5]
print(crt(c,n))
```

LATTICES

~~年年考年年错~~

Vectors

向量

```
#sage
v = vector([2,6,3])
w = vector([1,0,0])
u = vector([7,7,2])
print(3*(2*v - w)*2*u)
```

python可以考虑sympy库

Size and Basis

求向量的大小

9

Gram Schmidt

施密特正交化

```
from sympy import *
v= [Matrix([4,1,3,-1]),Matrix([2,1,-3,4]),Matrix([1,0,-2,7]),Matrix([6, 2, 9,
-5])]
o1=GramSchmidt(v)
print(o1)
print(273/298)
```

What's a Lattice?

介绍了格

求基本域体积

```
from sympy import *
v1 = [6, 2, -3]
v2 = [5, 1, 4]
v3 = [2, 7, 1]
v=Matrix([v1,v2,v3])
print(Abs(v.det()))
```

Gaussian Reduction

高斯规约。

高斯规约是**二维格基规约算法**，而后面的LLL算法是他的推广，在初期对一些题目的接触中时常有见到。

```
from sympy import *
def Gaussian(v1,v2):
    f=0
    while f==0:
        m=round((v1.T*v2)[0]/(v1.T*v1)[0])
        v2=v2-v1*m
        if (v1.T*v1)[0]<=(v2.T*v2)[0] :
            f=1
        else:
```

```
            u=v1;v1=v2;v2=u
    return v1,v2

v = Matrix([846835985, 9834798552])
u = Matrix([87502093, 123094980])
u_,v_=Gaussian(u,v)
print(u_.T*v_)
```

Find the Lattice

高斯规约的应用。

Backpack Cryptography

LLL算法解决背包问题，非常经典，另外同样经典的有HNP问题

```
from sage.all import*
from Crypto.Util.number import inverse,long_to_bytes
import numpy.matlib
```

```
public=
[260288377891444370372615148009023640057294926547602419331406531383682223097787288755377467188515435381259752760746,322734358011758862401399370931929863052553602421714393280581187496537763321855751120439457234561080720455397490349,8809235925640356478366528199313013354122660187796943690526741535304190975732474608039846124528182655242187298318401,60168470130011094592103693757246105014035295844018746759171550635943055833144080013775053870796901150009920943880321938146438506287399581527440417430588584840882696092934294084902945523450053657769621943658137961301651131849256211715106069147038884093417612611031254337545052481015138187405743501965632605638186210332229363017696976932877788761,502702742677974540308798846750017003106263447846689040491266463798703222616320168069962523670400796196343460832764,869898357835867381408831502013273741761245884104641886928849733342416815147023067163837850955640844995631528152465,515511378187957676256419959601984383408150348796281656976955880729383340611785836962788715725367023923811376366815,1198451789830250370051747325539317062840248262231767189821112135797070917660573203154198277815086909794051260620612,207867794910968434026003881920029657224591376925067493713968219177352819759854486838459675245909787840416982457750,23939998660321650302940254490061098488116010192329439679266520448622297542008130066135460317538477232355198015548,30666523613231533696157656609490848619698155697117217014529917438972033494026151238483795032177278298390345405872,55813028055082706821235257638771381102746823390517394468035556203781525740344611312889593732641294085958820436196,123471925832174980344066571541132411467266736109103860421447462536930482316849470378251137263190870093702164003085,14608970662901214238466135098821688248391926467312962140483133916656605646957208775974885408602335400264192368939044609789268438921971974291437386745709995449944982460253233318116903824908139575898313390656484000096200197650605,204029934276059225352901134714823317920576872465404508059719045291560482057171052793698580294637069578017200124432,41233337314300045774130798847005550457667515129934538773369261821827517702764378588104201854646045241850634196735617141841394029936032271242300411436468186527605778694791904388336630256716986959229015155926929044656318555335008040159343733741111425857826822378418279506878556410172233521573659129230160207775137647788108734681060204171716310420400368854382035433711393849497931198157457142475688392885528692673457879040032229126204246665421237770883128934755612926496986208337317871061684502803594375654879680702581403987248292734014139717756900004905653768133795128973,462785612281910846822645629160953231999037081137615204334672445418078666580807008664680479418625641113161518948781377961961618173276050791733447969083544152711482614563228085622136316525792569658878271751219358260960116292497570,5177893702214354197765880874906789918240219279453875332830883887904829133012817331154586014146682064325129989045162818703283403143951506584829326991145817432002799962270995307447547502891020315185637619750246213472813741620448776027004932547982341328939358509958095476626404677370071976476973814309636936985229627334737462813959367878361956751783883592777615753816019721386938304352886114144899633793990279753886017147418768318957094971059092135793030255036182790164206728419126869559412041581720253478692433039242122182936154601076445305192881487670023857390768790807560111712060813075236908220667610736435034720828632311503693977732506747336446543889835376509376627751501002198899611659500088905116081124903459987655681961070779401661280058520179333933249583949577952650461384618721593749731889019913528498351506231998813663610817085259159886252436377787033188821617058222086750004255773727241122002933136708113691878911208323578123773007930578262037899496150528209096244844693162873175197052185310868537643361362045652097962797444120544194231113379064789722632038820534069525681860876574626666231449964901398203572973150961359109133471921656796738018360295993368661727581587993987025833267475534534880245205825678851383794112621923835270816602222640451508423589645120802037884534648833197785178220474807186408588048378860572645147867426944194197351,48627235733549250075395637229925579860357539269701845180077442775272431
```

1245532865565077769183050844197681949934826 9,12915332497480538243428511854519703
2456153105619530812567391561913078099227042076507810281291422257016761595305 0,52
0707501920546816250915326019351261090208813534492143136485743644939372232638461 8
0262570097880176854184262464727 4,27235945678872169261876861219022245330483893491
6628492701462591276450281926223118982602858211688086607842351391495,119534191144
3971643274173975939640214774886833112156447700106417457364800390942092730922239 5
9694752862193314087240,39494513147060361437976795970465453802955753748931624609 2
9824271076416174795454888435359295374985464321232874864 37,39597942847560810176 52
3032821827462598667411571205176490373259301845426401778134019979554003928525751 3
438842708672,32210162949388722015919901958281089241895794194630075224524946209 30
3669703516221255726147016852295343534190529565 0,60610073299031334532969727880668
9890468389260473956139814736755054425008332441378632253987820295414394204036863 72
,4925824318350056214419228999956668064994376110691930990722479185970474150206280
7841084911994560885408004016369937 5,35629061412444807786488413692240929161712837
0298210212357882465167338600485728936925448944675136056707929560080237,469737185
5788791223780169597592974641322724324257452721079985341970149402350183353498863 9
8896979254122985841196030,52287110723491802412876813631512349725190227468111048 9
3865949443871812968260242891634318809615063145809355677439 10,4071517236124813917
2437542919391728962366949627802898229708645806211101295843632435052730286553576 6
565677711383191,59735438577497071544879774048385611913915202183491185214449029 87
3633035411848248014723728049130502971032683727415 7,54110643360821398560791312040
2276000940203625086988929757276286018099336445558864548353610869729642196223750 4
68493,41726995928052854815694899439726297305782105510828856509111374540973017462
6359955737489143948177504667498654245449,16584446719985300218164751678681580141 3
9393631889557208554636106980667302086572228222694577136665415558206089084 43,5487
5733171006797537647859403084623422036246809497621662400918381496284440644503330 4
1166889585888493324832898610 2,46581905044185793421090630512737437729185045070790
6416261994960542649394393702032587209990932960399224341143990297,369322923825463
7157244114044444523601258458656586739472423619682718639440790476960876217313112 4
3573179527276498509,55315878174959121195465967117314576794989779528732567793837 3
7024432651384567712647112325884387860427929689047327 69,40981201393816570088751975
8386718364160025926340003407045361393371862966914817952304595560620453598830906
305966865,49465486813875755276837163941823748926409947189441922027314750362407 75
6486556366191413600365682565704428450334644 8,58361329525246099314440307413090162
2751986348055784728175987246652496523293580989652454868505577305787293683850652,
4562309840816839876997123938749592898083555572156484700905979057515877029543042 6
7902007732742880873311096993362 04,39196430635656777174378129146834600960125068 26
6405306877726260536750371354188413207203531511343645151492477471286,269811462520
4699602885949533577793325415155634948064997054550367166896940557410966269271825 5
8039773813984145657639,56129158162087034209035841739296133948708529713411817898 9
2872710977041820807823924433164052250742341344620341779 4,52421010723975028824953
0336771864024916995632570549267972428294539507299820629133801771958736839361325 7
98918246415,74499040113803277306263886217659673645883223840279171192334357737741
6188821606489681769747549050845761848047743 69,53756608568908071710887064670545 83
3816343707543304607784599962203587946363677666375944798588496018116785741786051 7
,6705389018170801890916168339326153252699357872977055474102148284034829986692782
1016301415949708659944497709907470,22668729154414927057999516919896161740719023 4
5785167322377561172578699294344348898799732114443017458200668708690 34,3011913056
0797352224094299766590747178156378314088092947830899847927767559391822485618397 3
2773372383419543550017 0,27355468507806358741567075772566350813049875199811044280
7136494763920302805098071555958936900406570453984774374060,879802777435801705736
0711885330022447759523390238934386366517273834796726808965573602934519476728070 4
236057718111,41532511586334679129823293839341139346277745138624384282 8305531216895
9492635364694849768088353936060832360397 5987452,29186038199636984996399787574971
0331697722876276851205203280910491894467229365951220031470367159168511107680106 2

62,554653569462940342418063467925252548314485118886100002832290030505991378878498660088540140703141291011055029173137,3231897743846008346250132680849157689168552097465685515951585218734060915676871946742137654282385993172058115186922718058858959590973147209801344076076453248204179752381698740504252799624785795159692265638511254810000349196674810,27358050424415246906340567022795198030362182405787605888497833118825782149685233459905002020799012734835996511346 5,899940801542006857176369300683179313259311687232378991441663125289629570428421979155300470178930885016812158990951799035298060435050325814949085668466597731170494010567676699433302299350078224375491314709778102611124852540943861,337553339737054880017288314951575451797426862530219763936855885416298554494199226261714888518914541341927073075939,555767235943468829145176169155092609154443087625514005602174625189092890554469408093908780022725822401595827206530,167482207681968589044999185247091727351665495150856890489384055491411212222015536860601728784744556159207236698 01,317380564633191615800168658676142557493413060315417096622564923156521630376263849705099633192222625110143213444115 3,533990888376667129575141849433166253104032964155895368357797314378260092470904627861359175864364684662961150582207,513396659995631195176092161150862720525013962809253546948044716295216394348412814229843485871807710992091847490051,598751671521816401429095343374521592165563401213195481604556405443389323390172923217639290327197434030974530635632,502516418942980462174586089858060912235797554801782186782319843655355616321036648106166017773986280053024012403712,967576970849562460100258201072605387068271631357488091429989373624571694710611082922970667690790208431973613233961,160715027762704553320571142674023737670353756130518440136900430091151963142004047232920245715827837173811719927140,279138292123840748082780689543574043699162822819208361733228093396335579794292477744981338016264347327181324984710,764458420546893245235144216810982618575148276313646952559594185192456125711991234992057527291243539015482866 71941,38367531941413375363512191461521846435822081420874771201610356247615746494489713175667516814084618962948566478704 4,260741648290568813857849033448155840373964568801980310694295413631289231242930901519918814851819352903132884286000,5728151449564743801336207976761576542857746332994285342052418453357830953266311331951337985833603960670313095780 73,326258465939147178368353573060965288327891986807699582822092415027094204965326681853802159504539722937811913340954,270266570242986488258809014590807152136633692716132669770748395523214017062557603428657196661342410476403164567952,594635668324174018778140793057815156885870465660609865234586849536688338135131804764199647040009222634146148815637,112066852946512058163194024984815176069074331367673763590415760757313750687675218022751871678411881684718198988959,726431402519735935617000858215701313909147431217548685775021109040919890897082014369842428388208060971912252148 58,418558767829526524235103555737958351573183096833081038769308995724925326439890724874671213539641031754157727776067,196559288823369030489094238610617412012659194878611686482089456487889879135369906410569754176462601644487717691079,484475844260869041475828428835126624027291693283800645559775410528136122290210564467730445814182429120097372738911,3978955315722544232253859756188605490780259920593799714805266159422452452838181490656057664950910594775446176323 03,173098235745543952336517747078283517802667869630628062474315240281111485771833849083340162673485620557610425012773,39543874473024181778236119625568182792484704102866489650346068104122687197998641651420318998045617001312754906231 9,470021990867207717347003710359490169212637212255796418181420825247262094876084196634243149241752002339736588912053,116393009019558569654503508922282193810180596603376432764270301486325221610807518426481578453602546466299515294456,3126792363447388748142299792434626394865944533930643126711490098809808362895644092150885415099700230777392052034 68,125633612607015147027292740679836345332097512816636698981581758992992116056276272361001165705597842757882238693825,5505457476505769904642658843824992742548723119863816750907518868240378112356250952052178454518913965618934927153 91,582344947379262203945082609921047126789902458640974947 17

42650993237287005960795971391648836193471595008872938599 13,597445807393853093495
56486608135912281434810547891463825859533951516898749977166492472898125007984719
8831836930965,20308610071032279873771097067197649738932976573837729229038404179
99223838133909077953424675825393976346220002638 4,366083021996787911206272856169 6
65720981308167177143125303074466648545813452157612764258146407782634619278092168
081,56842506776187582319889359196675746133847070067561503394642914948397013805 56
65377562238998722395767377075284081587,29206317820241018663144351913867443664516
32334111619370856298560882590508273829850935068927636173020077591210377 31,572237
52094357584130199836523894041292898261733576815539469156709259569494329093827846
45330992232732142335071062 07,13073093889268689210763026272190124696905231813350 2
72867198415762917155443525150631287804049976192266530149503098 1,1851171081483522
76973404708807613996548096583954940273525781406848525491758486946236965943611210
198389159091280333,37060990092986925132287820152354618271473589014825595897838 75
36323150071727101545618799175517051946568254565710 32,40339673077619487045919962 7
54412263601087076825746335923576677553388293812814611283848957777749743220302003
0499998,39051905321921342230559910994741404789559080879636808534286046891726801 8
31063886439219937167927217463427841087830 7,
12844478194787359260260941878305571573687655772560893230161329444693493093347401
40200414348318990643165522646142 35,54329137353861345515580924849383043252068033 0
96133767779390522092883835232251456585145265044151848023472989215378 0,4885144443
83813071753894478409325136755661751625837651637348989332739608743318097848609715
93136271845090065971472 6,34558458242947542052620838286382645900548345520965571 26
36957752389218040279848223862500232738960994712140028026289,93010878843154734421
54356126519654880656208192303707459645905268663377572317146608812626982205731539
3084026072218,12533412965882925987419497258660569237455714460582608620237638858 6
42686843645624645184949324869641399446820464020,56277003203041404755795290491012
60272154560253435303502486168159436652560018077801127546607476458984432187236 42
72,12845170507087105615739691059176629603898923579826498243476925614411571260864
89372222981670665175567740623114203 53,49027896143426703969370679588881765338558 6
68950184827116534512192295631750414073242154602049467548246455041047250 2,2122875
43946551782522399704940695532581109453008804375002654843122502975490312129477869
62199808027768267419904603 1,35122816732913895712859245476641114260983623933047 93
31051630155591459798299725613134325016512314887321869487481161,36405658010615810
28956945712536719435719169208857951429600903117224442692412479630098145881998740
30295862636577768,32341061317491212886517476894909278097964617850503955502519436
44199904422199419487071174576214004591112315566215 85,55597945947531901827610613 3
18957858996468737377299554942381390277330427418444888565157000108361405414069206
3026580,47164589688818384887991806377009191765927090664881920190134665197595717 7
95075358309904758730448400641371636208706 5,59574610790289827090571463533907071 66
51708771264047581902664532594897071557252807014533004074458867603957329534516,55
78165176936033517196614110541443742502470406722269345346041513999027803191980988
21629853612396635344596388943480,75653615683769023911143698869320584951015514055
69726663864650736853084103563156083319828897797578247151755739409 2,3867292188623
61591185009654369415880766336899946663823664818477204172007165198875809899277634
66019079718502557961 4,39310826547794424066130845555061279676920047049850270390 50
73280606596277788078742986164286625262059483908055127428,36506580258320445000443
56619125065925324687537233994067406635340702894044922936807640786595884542404361
60849321237,34347479257585670008072639417708313477107942679804235919396610970085
05314080372454251733077970506766479339 37752374 84,44927058361022518091445278454033 3
56263157045399588599240993505575899417353399169528241020063502083018761244405660 7
,15247714860800097394008553226731949293262960919996421716727327931510940342643 44
32473053141371160594251975646390787,21575804681052002917141735796350854972686583
88309309811744956439557195065713987714479500497272342583058852205070 20,388644732
07957047924989481459394517730968961338656650829233609890799223999463537479907000
33033749283825638774943 12,33174396496627497383579687586254392056231321534282758 5

87681567913835717050445163816449882425899904436708697640574,29332835696437595107
22420729768512671868282424680187078105999073365253146704505026815222838761319240
77746023996643,29280448628075350402667475779416601551959038550552893714818494572
61793201373914809448361806106757179066940425104 11,27831591571539952405593680699 6
90709293779446705474946215046375615217684761739555711150830685146538646201126238
5630,10388404057729611948601275482246668222402537087291693949015931950042105893 2
99942136537773819300242176709717270634 1,11146365212965987400691528817483165463 41
46152513640366449316440114829594116719772451443937868409442532699879776869,47515
21242609697972650604533544547991248457174453572390272495977860291563074886976339
98763174770332805926500738683,22059733594411364313804091001926331825161620395454
87246609533039150892333013545115426622257513595735924065671257 79,460838912228809
94784309498615478069484131408768537935155110776371412761378932385879500327595835
0186756130179585099,14018310502444461951215872653766117189818438056807016123113 3
56761067988558487342665252182796195091140438391256162 1,10025831236373214993165 65
49158547430770829888011033153048299126820116382987576385251423248018523377569893
042593237,40529086718542059397271109204785840343141505895764810884829071285548 62
05273135789994549738296802436972506132007215,25695527706897458675250557070315305
15826828513980120776257218808521406282624944891589766798417165407061559168710 83,
59854915980295871040136283948128027368193395784194466208814951251847657300001180
34275136959033732483559806924463 93,30826328868101680764171440443463087748917675 4
88416404932263627403607691660808972101141818927437909613329077896797 7,8342859679
41017963172950884214733727802597984526821205468395186969062391741324266787643812
02145566082239505146 53,43989508629472834245444912695594189084482853491206487735 0
83037665194808314659173707148819625311625862934471746625 8,9188122612340725953692
15484341743828410017915681692931987699401312302566118066010584711058852546284224
99512141440,37726632436376626340063020572473121887724398027702520456725570882874
26128951751124624765487640418089984725157416 45,11667306253349187368118513103493 1
58057226285275103392914486800094138067494280052320927687535673346359235160344868 0
,57238242567269156027816815706946539463493497634492900168501163766058930300567 38
86165527821945622040251168934214 10,58977408651737149864366974706080289686150324 0
90656935701314862102828563998078554369065616283669488788050137942771 9,2991256261
28142030020988742420785075132372751191528474146303145649473683269241675130370288
76889992053128967424411 3,30468839554766611189810966333799291755735296874973012 55
49180444196974698222351897080702952045364871753888027443342,48273985167682410047
39204093472158483987893189001175614652973996141156667386144772591954150152721467
41220074932513,22354686265211323693586255615817790180380622973999495819595812770
08301253197675341793480378009197143286498013623 22,15042537568972520687117772748 2
71762542894412145621278847244692256411371851886763685550628057864190425988800603
8685,14337448307912234827477101516287274726388310521167594144048052430591082774 4
16893157205169122056113677539895765 9,12863335115803345379635610856097024152 78
89904619011394383277988372280437398843373552825146090070247278923404428730,24962
57016212615444381831087112057734789385606405712003251272524857794817010784527595
13943692466279038851599018511,33009848976287187977368101955973226246617201877327
25823086146726716710011993078655185068355193606939275798481321 22,972725709792065
28424127336981516817168566955222510512261839537633559389914877185855268875504270
285494647179225542,74718841026645027941391238796126141775030441881552798010185 59
51538737805244786742029656658887387302285770641110 32,59009205910055868684561742 5
29451214311094377006520731342399475542159755492342086349692903126315766192176134
558364,14795410687202371395146314569121647508443000630606041622136489683479576 94
25749212897622105818492094458111589403860,55599283027193617981279955000281341253
93908443074340155143272612494728237628012086452408067247517277892069584974 58,459
22343868855957124911668591464945009554012166893325850760974660979437453944806346
33265917492611911923708156621 17,57139320920091264882231218363705459881526939767 8
58061376895708911676548386512116249591826993515228832218764741125 3,1772861868240
84038346767370297094817293812392957721642873053028629715330336525966361030541938

87046542394424132410 9,58749126711314220193359085541298542925394865267954367292723278083703922366553917759387943826295988476862697992502 6,12107371999274855884928299650270344627924031395682365061968224086063037363494879869552351408587931043338876929791 1,32699282182187935416550269596102824008497829478738395771896393007077637284530541547061397608843693575104704351251 2,55897462658973985554837453480984923331777372313619418297379632868358904708526448610515770876401568010074036247,4742815171110808975425578458652860410974576502497279147458764961398827774612270762720589493061560015437093566148 27,40880447006931568560802817837347288973549001731224760995212446282117046967004745589464560120352241602331262757637,1993775822533799784140815526643457383942262483834864234777068575497020595546940372649587196444829868377564966132 46,67583806809325529684782118654476643411516600285151896093983454855502714712133346956141976654071062935812737453191,4525463419884391939822972140116787662585064902909110660902906476140684551518066214097566464305321177133334198142 00,63154079944843452528208874183624055953361990336542165468695871390964383215223885775202331596927466794955939855669,3345510339425835684746067418392139571013835902862511551866685432359209758979317439283576314534339348087967033304 73,43700012513366071240378802599220509069848443090765789406627207129603548337507847426022868786544480241606396763496 2,79996507523856267942889507576300340014719316733731500178081582238768493408405645914333660158893963260211116177267,1369572708243183410271249890342355858556469810932814537611454614408909555037936845171868759952021440272653299692 01,28020475319858890627598031839847872928528796154292028552997981227526631658010254587358741643340421270377624572 6478,537734235993878341769434982550042490365981751251428660237179942734374485415922424357453321846937022328664895920607,49835725687894957185424880462237093285992689499469012052623582488308375376513240186360550089209001676420693969875 6,59318365869460801409444910424977186587659512136720965625047115877163248639253373091393239350451398851219499423512 6,47152504795897165520853410705228785391394998792647667619751431032040411235020283503103705707957701802098089852040455,51555019552208634276923273952075076834560185097632001431240587694369170037814137715141409108561639182461304135622 2,22978465476796735514990949770981111936856065403720688094403522982769101181501691313111942245104382098092635394172 5,21716965401505128523855940357614751822157357430329104772981371096072579289255044572046460547617466380032817759745 3,44586555525410112782995864210267592768716871056970772546728610380393834811692683283425462408951948273855028080263,83946997792088073746354410376458121354546477090285151121896293987266118404260723878401677521317330022928683440101,47211935486226326843125163343242497690438421060339909356880629186233204831028205010084220412539647210131962031302 9,46843467515693389983627938872598324284244171067988563260495985345821466093790361374194115630948136965603015643581,27730258912679936098275011160344236055505193463675617106642488473249061687496289298000563796833648627737129810528 4,37796860324947087933757452089444569583341754367174335457777874936449439863762482510080776848131952814291888228252,32920166263148351927585020804342105914034742046258026081821605130797725513945495680568301003253822500829075333906 6,41095826074481445563790831716097933388154531407345762155920462314534468727979110329056723304867359444176833039156 8,39118406915003960144063906755718486281699105152381713239666619055551210638291990484889522432509871123022132816889 3,34177818015595568864982727157769026925392436710635945376806206298319430276614499669223353058511687034393954934404 8,48288518489189102683254301968062411233305196074641533123419907555306093358163048070633042055201765089231822542199 4,22741702987960229191389815445435046533419227545598336898099724394637106776612186294912508849693393305349330437508 2,13189105907717382348068168327480929670066701205459501548932979856766884145588227854043400661177825435146931575683 6,10397768540057593687600724535108042273456929170954015262222248308684001121180848475883988904526640536283310057221 7,43003969042086286471032886031791625155216273853846013104529538899048662194099926082062994680728312955050379104236 0,33605403934177936907875598161833872756742173925298437906008826456505206508090280066460595250953964418593702321038 4,4146504873015201958

```
60820485747902373712957920758077572646321108690388934071745453432265035539090489
903222596288408,589576193361941267176015154197092338077060428665767302320550323 0
24382985851379047593411265195718688560873123744185,218382333622730104159935425555
27568418203889486395199238424953339101509809368662516259889646157647721595788622
14025,254235654318169881307595715740138570651246806367324107684419478290893788 08
47391489213422972872487843717747974071,190127129345765908103303587019651942466 07
39328848462712905056740200333338683330000977323687164391887007102537011 2,2614594
49945270346696260426170010104493420330959761424072408598127181246567262293489464
049721489266230568086023687,39305787276307824937787063404299394225254439313697 83
40205701555086856991894130814830449765311294161681995357980571,31706670785655144
48925874421971725345587317548608849844635725162882472565389801781786630377526238
3346847940227722,352845629675989592022318947558037109666715372268243939061740352
17683305042078375467766641187687686522644881564342 0,579523499570692157776642365 2
78787278074363193157128877724940050501652213832135926670258239249988403301949338
255538,534781322034571849183222718240938369181782069830117215874801137890227720 5
44463940037268498986061166881241864175911,293947547828174245724554745263997068 01
69961778894705033835280048055596707128026407254693436168403671004431535347 52,202
56488447976344493484944853334005566670073013412177398480406734598723283264289836
58747426937025307701578635930 5,475307340957345844876811923970449788514706891727 4
80716267956523131203845997503382023500463149439850432076379159007,95321937770315
014432564328705207432344918409110542447836231022071623884991440705920244408120 57
106927678514406207,303764559063992561265341812276928855532662836999130994492052 4
85066252066328276934661336448618462235651452886616 33,310323302397755654510284518
63113807998143926563285268485287625411698909144539348757991175725604357001837723
0904180,407387187512823516321154849212634322952876110252179375736935664859854509
48882614204990368399161753825949446198320 6,211765773488300500716796064525502573 5
90145731868562963063378748592341237756767589777342751660513980880169703658019,11
81199968505698124437993063068750482132096860439876659253651297117423008440600143
47898233682054000714610165352429,456288037921986114882644161559494182818651772 33
52412628007837766962098777069066440691808672075550699370136864212 47,321798425169
97116991234329596269708557750807657111988819628911318108001381413344367322104986
035499697991535328417 2,32497652178923291184833750584128497874636153691590397101 1
25545143867352250073053700513718246367837289731419898859 5,395621759076694189110 4
73461483468243816716472466025836871653502259071450104902960119128530517955567830
675053452079,539300517585750216948117617165146582589224695990488749904551961039 0
61424290129525221984586819908097960720708938354,292793021286074222502055495200 59
28206951855928421958260548741314278182227610637328943226213363505359939112492638 5
,55404738788926538486985891647744218195240359725055594839294946929667394179338 18
52004501421929101000148453680659392,11778082542483728849447900938122175936115148
72394438211331024148888641529047321961954738130067624206469983822586 77,513764579
68198827042541863036571261307390879876995969073999879284617365021150807845801145
67843633129990856496154 13,421686906289957894155024887354760839265000904451245772
17530813113746727520248956170002165985881987360453865048999 4,4200378324232595253
88141394520857134457021929872555809167052539034540217718781279113965175987358081
438109891771580,364516057451120406028049542359394620813467917703101816636316990 5
40484148358389564090556409485819480160330035113 33,658664434698662488281190999945
18897685990064406903627156894902667947376070679854260383038634727146436274230980
496,276764137014924477639649452057696027597683476237411899802782259437285871879 4
02710506340542175909426595423027223 34,500312789935788689187812810985806111797362
02899835367784381912548504557694347290197605557966366526790580982090586 2,5200643
54401353505774803720281331074080600746212325401527048530022713769008774050816490
54135614235475780559527306 8,495854656037423684061417113244964481431602915324717 6
05570975073575414392233479237472936965636133612283412033946051,91739870792230359
21004304640178695919004592912414170965387369939857407757939578555520046273450972
8806350612588545,484531754577892922131892661653620989224382080321025512011181426
```

```
67844254791296457322304851956608558262351782586541 8,1127146843440843910788669808
392555943551878853397017157680091535512704323228267159699897283409632136930958 49
427668,4044292047237865342995253331221633425885869914219024668398084684874938963
309798734161059088414475354269236812209 57,9240474242421764004037536253244417235 9
091402942418950195520660310216430170054358290537973281349284862065214755739,2240
433939690430135325118802230758091208428561656080866929281124301715485694933985 51
019081676395857489451126409940,4305919427803364191555497499680058924116536587126
751817219863902878291078989381194676206640960307162723876513248]
c=4569075283329962627686056584893018330801694678637585980629434662274508251251 18
476988969148430235585605098782432175 21
n=len(public)
L = Matrix(ZZ,n + 1,n+1)
for row, x in enumerate(public):
    L[row, row] = 2
    L[row, -1] = x
L[-1, :] = 1
L[-1, -1] = c
#print(L.LLL())#人肉查找符合条件的行
a=1011111000101110000101101110011010001100110011001110111000101110000101101110 01
101000110000110110111110101100111010001100111110101101011011000110001011001100 11
100000111000101100011101101101011011111010100111101011011011011110111101100010 11
100000111010011110010011101100011 00
b=0b0011000110111001001111001011100000111010001101111011110110111010111100101 0
111110110101101101110001101000111000001110011001101000110001101101011010111110 01
100010111001101011111011011000011000101100111011010000111010001110111001100110 01
100010110011101101000011101000111110 1
print(long_to_bytes(b))
```