ez_Lattice

主要的等式关系在这行代码中

```
r = my_mod((Fraction(a, b) + Fraction(b, c) + Fraction(c, a)), n)
```

转换成数学等式为

$$\begin{aligned} r &= \frac{a^2c+b^2a+c^2b}{abc} \pmod n \\ a^2c+b^2a+c^2b &\equiv rabc \pmod n \end{aligned}$$

这里因为n很大因此可以打二元 copper 或者造格都可以，记 $x=a^2c+b^2a+c^2b,\ y=abc$，得到

$$x = ry - kn$$

可造如下的格

$$L = \begin{bmatrix} r & 1 \\ n & 0 \end{bmatrix}$$

然后规约出x,y，求解Groebner基就可以了

```
from Crypto.Util.number import *

n =
230753139895299023926292215505753387661263695273485091892042197452275255846185313
200348981966907835274611350438343928713551752466731879758513653579074389959176128
831284513922204044608539441819333488590113877699025419769818109293404775473030789
780292812266274311425730129884131966718219980953383772482675740504354146238090948
810049397214605606669249385142058980568692504394540545601354497674891385185120818
931498046615195290260581428194409790592838703644581787396818027416962668787043507
377187797360709489211401916923704348524317894031645965377568625713853617445422164
623289615002075173979723949614549209805804788124769545877487914108287103357256306
422824914126642665015465711681230486812216284313338043359375981621131119882932095
812948327470528234652870775873875981064550578169454223158036579067572609958566666
722316634938406741761626290973681206244134762450852216394819385605117212964526715
3677785486881387823797678085115531
r =
316357730244990138318480392920339507953599774657318652649725998111060415837780679
009999405269140966375000515906560619496082571605663471631131470275663609172428712
257644205939983000602117636841042094137909270994489006180702241636182751458240703
434556718405220771794328551245380406260291895859963633970184705015945753361239028
118936164574764604093703767606098157821598357174568536818571621524003208204629066
266122553554364682909027455873000963705680906406473673948524074362921537706394845
435596305922365476386783417882396612838670750361780239828705543155620906742332880
907769333151894684047288178945475192381469701918877050545060438654073227836562579
092510733360041641829511301296938302685612597494829174799817095624892098946562728
989788700063992016344013377106116500089012796209682182790265326810810832996222473
181530235838112932995792432175498244399830592904468712521632346822891848624250332
534504069706496205073958230072316
myprime = [864119, 989837, 698437, 724469, 543379, 833281, 916537, 864221,
920743, 906539, 878719, 532331, 694619, 769357, 787181, 723257, 812213, 983519,
737747, 1017031]
```

```
c = [423083, 495840, 544283, 571240, 289138, 194415, 271148, 348295, 209494,
533624, 530740, 519792, 673659, 533658, 765468, 193697, 258028, 354419, 279321,
855351]

c = crt(c, myprime)

L = matrix(ZZ, [[r, 1], [n, 0]])
L = L.LLL()[0]
x, y = map(abs, L)

P = QQ["a, b"]
a, b = P.gens()
I = P.ideal([
    a * b**2 + a**2 * c + b * c**2 - x,
    a * b * c - y,
])
try:
    sol = I.variety()[0]
    print(long_to_bytes(int(sol[a])))
except:
    pass
```

flag为

```
VCTF{ez_LLL_challenge_and_have_a_good_luck_in_this_game_hhhh!!!}
```