Isogeny (6/12) : f , f ' special

Toy Example : p = 2^4 * 3^3 * 2 - 1

<KEY GENERATION>

1 Elliptic curve

```
import random
```

```
f,l1,l2,e1,e2 = 2,2,3,4,3 ; p = (l1^e1)*(l2^e2)*f - 1
F.<a> = GF(p^2)                                                    ### Finite field : generator  a

E0 = EllipticCurve( F,[0,0,0,1,0]) ; E0 ; print('f = %d , l_1 = %d , l_2 = %d , e_1 = %d , e_2 = %d , p = %d' %
(f,l1,l2,e1,e2,p))
```

```
Elliptic Curve defined by y^2 = x^3 + x over Finite Field in a of
size 863^2
f = 2 , l_1 = 2 , l_2 = 3 , e_1 = 4 , e_2 = 3 , p = 863
```

```
def x_to_point(x):

    return E0(x,sqrt(x^3+x))
```

Supersingular

```
E0.is_supersingular()
```

```
True
```

2 points

```
print('l_2^e_2 = %d, l_1^e_1 = %d' %(l2^e2,l1^e1))
```

```
l_2^e_2 = 27, l_1^e_1 = 16
```

```
%time
l2e2_torsion_gp = E0((0)).division_points(l2^e2)       ####  E_0[l_2 ^ e_2] torsion gp
l1e1_torsion_gp = E0((0)).division_points(l1^e1)         ####  E_0[l_1 ^ e_1] torsion gp
```

```
CPU time: 2.89 s,  Wall time: 2.90 s
```

```
R2 = random.choice(l2e2_torsion_gp)          ### R2

while True:
    S2 = random.choice(l2e2_torsion_gp)
    if R2 != S2 :
        break                                ### R2 , S2

P1 = random.choice(l1e1_torsion_gp)          ### P1
```

```
print('R2 = {} , S2 = {} , P1= {} '.format(R2,S2,P1))   ###
```

```
R2 = (422*a + 27 : 548*a + 682 : 1) , S2 = (164*a + 7 : 478*a + 586
: 1) , P1= (197*a + 648 : 758*a + 405 : 1)
```

```
print('{}*R2 = {} , {}*S2 = {} , {}*P1= {} '.format(l2^e2,l2^e2*R2,l2^e2,l2^e2*S2,l1^e1,l1^e1*P1))
```

```
27*R2 = (0 : 1 : 0) , 27*S2 = (0 : 1 : 0) , 16*P1= (0 : 1 : 0)
```

3 Isogeny **(φ), E1**

```
phi = EllipticCurveIsogeny(E0, P1 )  ###### isogeny Φ
E1 = phi.codomain()                  ###### isogeny Φ codomain E1

print('phi = {} WnWnE_1 = {}'.format(phi,E1))
```

```
phi = Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3
+ x over Finite Field in a of size 863^2 to Elliptic Curve defined
by y^2 = x^3 + (155*a+756)*x + (18*a+470) over Finite Field in a of
size 863^2

E_1 = Elliptic Curve defined by y^2 = x^3 + (155*a+756)*x +
(18*a+470) over Finite Field in a of size 863^2
```

isogeny map : .rational_maps()

```
phi.rational_maps()        ######### (x,y)
```

```
((x^16 + (-36*a - 343)*x^15 + (169*a + 373)*x^14 + (312*a +
388)*x^13 + (284*a + 400)*x^12 + (-398*a + 78)*x^11 + (330*a -
125)*x^10 + (-41*a - 139)*x^9 + (-295*a - 193)*x^8 + (249*a -
```

```
353)*x^7 + (-321*a - 224)*x^6 + (-199*a + 165)*x^5 + (-182*a +
265)*x^4 + (352*a + 127)*x^3 + (-31*a + 257)*x^2 + (-239*a + 77)*x +
(174*a + 150))/(x^15 + (-36*a - 343)*x^14 + (200*a - 339)*x^13 +
(143*a + 351)*x^12 + (-65*a - 311)*x^11 + (195*a - 81)*x^10 + (23*a
+ 395)*x^9 + (-25*a + 252)*x^8 + (340*a - 422)*x^7 + (329*a -
325)*x^6 + (-24*a + 201)*x^5 + (307*a - 158)*x^4 + (242*a - 368)*x^3
+ (-118*a - 163)*x^2 + (147*a - 20)*x + (48*a + 133)),
 (x^23*y + (-286*a + 33)*x^22*y + (215*a + 131)*x^21*y + (203*a -
75)*x^20*y + (202*a - 238)*x^19*y + (203*a + 273)*x^18*y + (-348*a -
351)*x^17*y + (-31*a - 269)*x^16*y + (412*a + 373)*x^15*y + (117*a +
414)*x^14*y + (204*a + 157)*x^13*y + (-203*a - 363)*x^12*y + (290*a
- 250)*x^11*y + (-59*a - 49)*x^10*y + (-189*a + 349)*x^9*y + (-391*a
- 360)*x^8*y + (385*a - 231)*x^7*y + (328*a - 189)*x^6*y + (-142*a -
283)*x^5*y + (76*a + 398)*x^4*y + (-303*a + 129)*x^3*y + (352*a +
62)*x^2*y + (-16*a - 397)*x*y + (366*a + 237)*y)/(x^23 + (-286*a +
33)*x^22 + (184*a - 20)*x^21 + (-60*a - 208)*x^20 + (-235*a +
431)*x^19 + (428*a - 178)*x^18 + (-a + 378)*x^17 + (327*a +
338)*x^16 + (-27*a - 356)*x^15 + (77*a + 351)*x^14 + (-385*a -
137)*x^13 + (425*a - 63)*x^12 + (226*a + 372)*x^11 + (95*a +
156)*x^10 + (118*a - 425)*x^9 + (-128*a + 248)*x^8 + (344*a +
299)*x^7 + (310*a - 417)*x^6 + (184*a + 337)*x^5 + (371*a - 154)*x^4
+ (-105*a + 307)*x^3 + (11*a + 243)*x^2 + (79*a + 327)*x + (409*a -
149)))
```

isogeny mapping

```
po = E0.random_element()   ##### E0 random pt
print("random point = {}".format(po))

phi(po)        #### isogeny(point) ->mapping value.
print("mapping to {}".format(phi(po)))
```

```
random point = (212*a + 489 : 727*a + 28 : 1)
mapping to (179*a + 752 : 509*a + 812 : 1)
```

4 J-invariant , R2_prime , S2_prime

```
j0 , j1 = E0.j_invariant() , E1.j_invariant() ; print('j(E_0) = {} , j(E_1) = {}'.format(j0,j1))
```

```
j(E_0) = 2 , j(E_1) = 465*a + 831
```

```
R2_prime , S2_prime = phi(R2) , phi(S2) ; print(' RW'_2 = {} , SW'_2 = {} '.format(R2_prime , S2_prime))
```

```
R'_2 = (347*a + 480 : 357*a + 737 : 1) , S'_2 = (712*a + 662 :
268*a + 204 : 1)
```

5 Hash

```
hexbin = { '0' : '0000' , '1' : '0001' , '2' : '0010' , '3' : '0011' , '4': '0100' , '5': '0101' , '6' : '0110' , '7' :'0111' ,
'8' :'1000' , '9' : '1001' , 'a' : '1010' , 'b' : '1011' , 'c': '1100' ,'d':  '1101' , 'e': '1110' ,'f' : '1111'}

binhex = {}
for i,j in hexbin.items():
    binhex[j] = i

def hex_to_bin(hex):
    res = ''

    for str in hex:

        res = res + hexbin[str]


    return res


############# ##############
```

```
import hashlib

def Hash(string):                        ####### Hash 함수 : output 128 bits

    return hex_to_bin(hashlib.md5(string).hexdigest())

print('문자열 mathematics의 해쉬 값은 %s ' %(Hash('mathematics')))     ####### 예시
print('bits = {}'.format(len(Hash('mathematics'))))
```

```
문자열 mathematics의 해쉬 값은
01101010111000101000101001010101010001010110101100010000000110111110₩
10000010011000011110010111011110111001000100110011010011110
bits = 128
```

6 isomorphism f

```
from sage.schemes.elliptic_curves.weierstrass_morphism import *
```

E0'

```
E0_prime = EllipticCurve( F,[0,0,0,2,0]) ; print("E0_prime = {}".format(E0_prime))
```

```
E0_prime = Elliptic Curve defined by y^2 = x^3 + 2*x over Finite
Field in a of size 863^2
```

```
isomorphisms(E0,E0_prime )  ###### : Isomorphisms between Weierstrass models :
http://doc.sagemath.org/html/en/reference/curves/sage/schemes/elliptic_curves/weierstrass_morphism.html
```

```
[(422, 0, 0, 0), (441, 0, 0, 0), (93*a + 385, 0, 0, 0), (770*a +
478, 0, 0, 0)]
```

```
u,r,s,t2 = isomorphisms(E0 ,E0_prime )[-1]
```

f isomorphism

```
x,y = var('x,y')
print("f : (x,y) to ({},{})".format((u^2)*x + r , (u^3)*y + s* (u^2) *x + t2))
print("f_inv : (x,y) to ({},{})".format((u^-2)*(x - r) , (u^-3)*(y - t2) - s * (u^-3) *(x - r)))
```

```
f : (x,y) to (557*x,(842*a + 442)*y)
f_inv : (x,y) to (251*x,(677*a + 93)*y)
```

```
def f_iso(P):       ##### f

    p1,p2 = P[:2]

    iso = lambda x,y : ((u^-2)*(x - r) , (u^-3)*(y - t2) - s * (u^-3) *(x - r))

    if p1==0 and p2==1:
        return E0_prime(P)

    return E0_prime(iso(p1,p2))

def f_inv(P):           ##### f inverse

    p1,p2 = P[:2]

    iso = lambda x,y : ((u^2)*x + r , (u^3)*y + s* (u^2) *x + t2)

    if p1==0 and p2==1:
        return E0(P)

    return E0(iso(p1,p2))
```

```
P1_tilda , R2_tilda , S2_tilda = f_iso(P1),f_iso(R2),f_iso(S2) ; P1_tilda , R2_tilda , S2_tilda
```

```
((256*a + 404 : 23*a + 425 : 1),
 (636*a + 736 : 825*a + 34 : 1),
 (603*a + 31 : 164*a + 224 : 1))
```

<Sign>

1~2 Compute isogenies

```
t = 128

alpha = ['index']           #######  α_i = alpha[i]
psi = ['index']             #######  Ψ_i = psi[i]
E2 =  ['index']             #######  E_2,i = E2[i]
j2 = ['index']              #######  j_2,i = j2[i]
psi_prime =['index']        #######  Ψ'_i = psi_prime[i]
E3 = ['index']              #######  E_3,i = E3[i]
j3 = ['index']              #######  j_3,i = j3[i]

J2 = ''                     ####### J2 = j_2,1|j_2,2|j_2,3|...   , j_2,i sequence
J3 = ''                     ####### J3 = j_3,1|j_3,2|j_3,3|...   , j_3,i sequence

for i in range(1,t+1):
    ranalp = random.randrange(0,l2^e2 + 1)

    alpha.append(ranalp)

    psi.append(EllipticCurveIsogeny(E0, R2 + alpha[i]*S2 ))
    E2.append(EllipticCurveIsogeny(E0, R2 + alpha[i]*S2 ).codomain())
    a2 = E2[i].j_invariant()
    j2.append(a2)
    J2 = J2 + '{}'.format(a2)
```

```
    psi_prime.append(EllipticCurveIsogeny(E1, R2_prime + alpha[i]*S2_prime ))
    E3.append(EllipticCurveIsogeny(E1, R2_prime + alpha[i]*S2_prime ).codomain())

    a3 = E3[i].j_invariant()
    j3.append(a3)
    J3 = J3 + '{}'.format(a3)
```

* f' isomorphism

E1, Isomorphsim -> E1'

```
E1 ; E1.a_invariants()
```

```
Elliptic Curve defined by y^2 = x^3 + (155*a+756)*x + (18*a+470)
over Finite Field in a of size 863^2
(0, 0, 0, 155*a + 756, 18*a + 470)
```

```
cc , dd = E1.a_invariants()[3:]
count = 0

for i in range(2,863):
     for j in range(2,863):


        E1_prime = EllipticCurve( F,[0, 0, 0, i*cc , j*dd])
        if E1.is_isomorphic(E1_prime):
            print(count)
            count += 1
            print( i*cc , j*dd)
        if count ==3:
            break

     if count ==3:
            break
```

```
0
(310*a + 649, 457*a + 522)
1
(310*a + 649, 406*a + 341)
2
(465*a + 542, 349*a + 291)
```

```
EllipticCurve( F,[0, 0, 0, i*cc , j*dd])
```

```
Elliptic Curve defined by y^2 = x^3 + (465*a+542)*x + (349*a+291)
over Finite Field in a of size 863^2
```

```
E1(phi(P1))
```

```
(0 : 1 : 0)
```

```
isomorphisms(E1,E1_prime)
```

```
[(447*a + 208, 0, 0, 0), (416*a + 655, 0, 0, 0)]
```

E1'

```
E1_prime
```

```
Elliptic Curve defined by y^2 = x^3 + (465*a+542)*x + (349*a+291)
over Finite Field in a of size 863^2
```

f ' define

```
u2,r2,s2,t3 = isomorphisms(E1,E1_prime)[-1]

x,y = var('x,y')
print("f_prime_inv : (x,y) to ({},{})".format((u2^2)*x + r2 , (u2^3)*y + s2* (u2^2) *x + t3))
print("f_prime : (x,y) to ({},{})".format((u2^-2)*(x - r2) , (u2^-3)*(y - t3) - s2 * (u2^-3) *(x - r2)))
```

```
f_prime_inv : (x,y) to (423*x,(779*a + 42)*y)
f_prime : (x,y) to (406*x,(385*a + 239)*y)
```

```
def f_prime_iso(P):       ##### f_prime

    p1,p2 = P[:2]


    iso = lambda x,y : ((u2^-2)*(x - r2) , (u2^-3)*(y - t3) - s2 * (u2^-3) *(x - r2))
    if iso(p1,p2)[0] == 0:
        return E1_prime(list(iso(p1,p2))+[0])
    return E1_prime(iso(p1,p2))

def f_prime_inv(P):           ##### f_prime inverse
    p1,p2 = P[:2]
```

```
    iso = lambda x,y : ((u2^2)*x + r2 , (u2^3)*y + s2* (u2^2) *x + t3)

    if iso(p1,p2)[0] == 0:
        return E1(list(iso(p1,p2))+[0])
    return E1(iso(p1,p2))
```

E0' & E1' isogeny

```
E0_prime.is_isogenous(E1_prime)
```

```
True
```

φ tilda mapping

```
def phi_tilda(P):        ##### phi_tilda

    return f_prime_iso(phi(f_inv(P)))
```

```
point=E0_prime.random_element()
point
```

```
(839*a + 615 : 19*a + 653 : 1)
```

```
phi_tilda(point)
```

```
(135*a + 76 : 806*a + 440 : 1)
```

```
phi_tilda(point).rational_maps()
```

```
Traceback (click to the left of this block for traceback)
...
AttributeError: 'EllipticCurvePoint_finite_field' object has no
attribute 'rational_maps'
```

R2_tilda , S2_tilda : phi well-defined check: ㄱ- mapping , ㄴ-mapping

```
print('fprimeinv o ϕtilda(S2tilda) = {} ₩nϕo finv(S2tilda) = {}  '.format(  phi(  f_inv(S2_tilda)) ,
f_prime_inv(phi_tilda(S2_tilda))))
print('₩nfprimeinv o ϕtilda(R2tilda) = {} ₩nϕo finv(R2tilda) = {}  '.format(  phi(  f_inv(R2_tilda)) ,
f_prime_inv(phi_tilda(R2_tilda))))
```

```
fprimeinv o ϕtilda(S2tilda) = (712*a + 662 : 268*a + 204 : 1)
ϕo finv(S2tilda) = (712*a + 662 : 268*a + 204 : 1)

fprimeinv o ϕtilda(R2tilda) = (347*a + 480 : 357*a + 737 : 1)
ϕo finv(R2tilda) = (347*a + 480 : 357*a + 737 : 1)
```

Using phi_tilda, R2_tilda_prime, S2_tilda_prime define

```
R2_tilda_prime , S2_tilda_prime = phi_tilda(R2_tilda) ,phi_tilda(S2_tilda)

print('R2_tilda_prime = {} ,₩nS2_tilda_prime = {}  '.format(R2_tilda_prime , S2_tilda_prime))
```

```
R2_tilda_prime = (213*a + 705 : 795*a + 677 : 1) ,
S2_tilda_prime = (830*a + 379 : 680*a + 602 : 1)
```

```
print('α_i = {} '.format(alpha))                ########
#print('Ψ_i = {} '.format(psi))
#print('E_2,i = {}'.format(E2))

#print('ΨW'_i = {}'.format(psi_prime))
#print('E_3,i = {}'.format(E3))
```

```
α_i = ['index', 15, 5, 6, 18, 2, 12, 25, 22, 25, 13, 0, 19, 16, 24,
27, 17, 27, 9, 1, 19, 7, 7, 3, 12, 9, 16, 6, 22, 5, 12, 13, 27, 27,
20, 8, 0, 26, 16, 14, 12, 15, 8, 3, 11, 23, 11, 25, 16, 10, 2, 17,
19, 11, 11, 4, 15, 4, 26, 10, 26, 0, 8, 21, 19, 6, 2, 4, 15, 12, 2,
27, 19, 15, 14, 18, 22, 3, 19, 15, 1, 23, 13, 13, 10, 25, 24, 4, 15,
5, 20, 3, 12, 13, 10, 19, 18, 10, 2, 9, 3, 1, 5, 6, 11, 13, 13, 24,
4, 1, 14, 8, 13, 25, 22, 3, 17, 18, 3, 26, 25, 5, 25, 27, 11, 24, 2,
3, 6]
```

Sign step: j_2,i , j_3,i

```
for i in range(1,t+1):
    print('j_2,{} = {}, j_3,{} = {}'.format(i,j2[i],i,j3[i]))
```

```
WARNING: Output truncated!
full_output.txt
```

```
j_2,1 = 515*a + 716, j_3,1 = 232*a + 541
j_2,2 = 473*a + 144, j_3,2 = 657*a + 665
j_2,3 = 473*a + 144, j_3,3 = 657*a + 665
j_2,4 = 451*a + 551, j_3,4 = 590*a + 114
j_2,5 = 419*a + 148, j_3,5 = 89
```

```
j_2,6 = 696, j_3,6 = 482
j_2,7 = 633*a + 848, j_3,7 = 494
j_2,8 = 230*a + 618, j_3,8 = 633*a + 848
j_2,9 = 633*a + 848, j_3,9 = 494
j_2,10 = 257, j_3,10 = 232*a + 541
j_2,11 = 348*a + 368, j_3,11 = 803*a + 599
j_2,12 = 520*a + 114, j_3,12 = 250*a + 693
j_2,13 = 281*a + 827, j_3,13 = 451*a + 551
j_2,14 = 412*a + 139, j_3,14 = 740*a + 293
j_2,15 = 348*a + 368, j_3,15 = 803*a + 599
j_2,16 = 348*a + 368, j_3,16 = 152*a + 605
j_2,17 = 348*a + 368, j_3,17 = 803*a + 599
j_2,18 = 390*a + 617, j_3,18 = 406*a + 197
j_2,19 = 343*a + 634, j_3,19 = 406*a + 197
j_2,20 = 520*a + 114, j_3,20 = 250*a + 693
j_2,21 = 257, j_3,21 = 548*a + 32
j_2,22 = 257, j_3,22 = 548*a + 32
j_2,23 = 419*a + 148, j_3,23 = 509*a + 781
j_2,24 = 696, j_3,24 = 482
j_2,25 = 390*a + 617, j_3,25 = 406*a + 197
j_2,26 = 281*a + 827, j_3,26 = 451*a + 551
j_2,27 = 473*a + 144, j_3,27 = 657*a + 665
j_2,28 = 230*a + 618, j_3,28 = 633*a + 848
j_2,29 = 473*a + 144, j_3,29 = 657*a + 665
j_2,30 = 696, j_3,30 = 482
j_2,31 = 257, j_3,31 = 232*a + 541
j_2,32 = 348*a + 368, j_3,32 = 803*a + 599
j_2,33 = 348*a + 368, j_3,33 = 803*a + 599
j_2,34 = 444*a + 567, j_3,34 = 22
j_2,35 = 451*a + 551, j_3,35 = 371*a + 206
j_2,36 = 348*a + 368, j_3,36 = 803*a + 599
j_2,37 = 390*a + 617, j_3,37 = 527*a + 557
j_2,38 = 281*a + 827, j_3,38 = 451*a + 551
j_2,39 = 515*a + 716, j_3,39 = 548*a + 32
j_2,40 = 696, j_3,40 = 482
j_2,41 = 515*a + 716, j_3,41 = 232*a + 541
j_2,42 = 451*a + 551, j_3,42 = 371*a + 206
j_2,43 = 419*a + 148, j_3,43 = 509*a + 781
j_2,44 = 696, j_3,44 = 853*a + 60
j_2,45 = 412*a + 139, j_3,45 = 527*a + 557
j_2,46 = 696, j_3,46 = 853*a + 60
j_2,47 = 633*a + 848, j_3,47 = 494
j_2,48 = 281*a + 827, j_3,48 = 451*a + 551
j_2,49 = 241, j_3,49 = 803*a + 599
j_2,50 = 419*a + 148, j_3,50 = 89
j_2,51 = 348*a + 368, j_3,51 = 152*a + 605
j_2,52 = 520*a + 114, j_3,52 = 250*a + 693
j_2,53 = 696, j_3,53 = 853*a + 60
j_2,54 = 696, j_3,54 = 853*a + 60
j_2,55 = 582*a + 245, j_3,55 = 509*a + 781
j_2,56 = 515*a + 716, j_3,56 = 232*a + 541
j_2,57 = 582*a + 245, j_3,57 = 509*a + 781
j_2,58 = 390*a + 617, j_3,58 = 527*a + 557
j_2,59 = 241, j_3,59 = 803*a + 599

...

j_2,69 = 696, j_3,69 = 482
j_2,70 = 419*a + 148, j_3,70 = 89
j_2,71 = 348*a + 368, j_3,71 = 803*a + 599
j_2,72 = 520*a + 114, j_3,72 = 250*a + 693
j_2,73 = 515*a + 716, j_3,73 = 232*a + 541
j_2,74 = 515*a + 716, j_3,74 = 548*a + 32
j_2,75 = 451*a + 551, j_3,75 = 590*a + 114
j_2,76 = 230*a + 618, j_3,76 = 633*a + 848
j_2,77 = 419*a + 148, j_3,77 = 509*a + 781
j_2,78 = 520*a + 114, j_3,78 = 250*a + 693
j_2,79 = 515*a + 716, j_3,79 = 232*a + 541
j_2,80 = 343*a + 634, j_3,80 = 406*a + 197
j_2,81 = 412*a + 139, j_3,81 = 527*a + 557
j_2,82 = 257, j_3,82 = 232*a + 541
j_2,83 = 257, j_3,83 = 232*a + 541
j_2,84 = 241, j_3,84 = 803*a + 599
j_2,85 = 633*a + 848, j_3,85 = 494
j_2,86 = 412*a + 139, j_3,86 = 740*a + 293
j_2,87 = 582*a + 245, j_3,87 = 509*a + 781
j_2,88 = 515*a + 716, j_3,88 = 232*a + 541
j_2,89 = 473*a + 144, j_3,89 = 657*a + 665
j_2,90 = 444*a + 567, j_3,90 = 22
j_2,91 = 419*a + 148, j_3,91 = 509*a + 781
j_2,92 = 696, j_3,92 = 482
j_2,93 = 257, j_3,93 = 232*a + 541
j_2,94 = 241, j_3,94 = 803*a + 599
j_2,95 = 520*a + 114, j_3,95 = 250*a + 693
j_2,96 = 451*a + 551, j_3,96 = 590*a + 114
j_2,97 = 241, j_3,97 = 803*a + 599
j_2,98 = 419*a + 148, j_3,98 = 89
```

```
j_2,99 = 390*a + 617, j_3,99 = 406*a + 197
j_2,100 = 419*a + 148, j_3,100 = 509*a + 781
j_2,101 = 343*a + 634, j_3,101 = 406*a + 197
j_2,102 = 473*a + 144, j_3,102 = 657*a + 665
j_2,103 = 473*a + 144, j_3,103 = 657*a + 665
j_2,104 = 696, j_3,104 = 853*a + 60
j_2,105 = 257, j_3,105 = 232*a + 541
j_2,106 = 257, j_3,106 = 232*a + 541
j_2,107 = 412*a + 139, j_3,107 = 740*a + 293
j_2,108 = 582*a + 245, j_3,108 = 509*a + 781
j_2,109 = 343*a + 634, j_3,109 = 406*a + 197
j_2,110 = 515*a + 716, j_3,110 = 548*a + 32
j_2,111 = 451*a + 551, j_3,111 = 371*a + 206
j_2,112 = 257, j_3,112 = 232*a + 541
j_2,113 = 633*a + 848, j_3,113 = 494
j_2,114 = 230*a + 618, j_3,114 = 633*a + 848
j_2,115 = 419*a + 148, j_3,115 = 509*a + 781
j_2,116 = 348*a + 368, j_3,116 = 152*a + 605
j_2,117 = 451*a + 551, j_3,117 = 590*a + 114
j_2,118 = 419*a + 148, j_3,118 = 509*a + 781
j_2,119 = 390*a + 617, j_3,119 = 527*a + 557
j_2,120 = 633*a + 848, j_3,120 = 494
j_2,121 = 473*a + 144, j_3,121 = 657*a + 665
j_2,122 = 633*a + 848, j_3,122 = 494
j_2,123 = 348*a + 368, j_3,123 = 803*a + 599
j_2,124 = 696, j_3,124 = 853*a + 60
j_2,125 = 412*a + 139, j_3,125 = 740*a + 293
j_2,126 = 419*a + 148, j_3,126 = 89
j_2,127 = 419*a + 148, j_3,127 = 509*a + 781
j_2,128 = 473*a + 144, j_3,128 = 657*a + 665
```

full_output.txt

```
psi[4].rational_maps()
```

```
((x^27 + (406*a + 202)*x^26 + (151*a + 427)*x^25 + (129*a -
316)*x^24 + (-4*a + 282)*x^23 + (307*a - 128)*x^22 + (-381*a -
168)*x^21 + (213*a - 303)*x^20 + (-42*a + 167)*x^19 + (349*a +
165)*x^18 + (95*a - 160)*x^17 + (-372*a - 204)*x^16 + (365*a -
90)*x^15 + (233*a + 88)*x^14 + (336*a + 56)*x^13 + (386*a -
408)*x^12 + (430*a + 338)*x^11 + (76*a - 3)*x^10 + (362*a - 349)*x^9
+ (-172*a - 317)*x^8 + (-201*a + 291)*x^7 + (423*a + 218)*x^6 +
(-309*a - 123)*x^5 + (-79*a - 266)*x^4 + (-360*a - 16)*x^3 + (410*a
- 220)*x^2 + (-188*a - 325)*x + (87*a - 282))/(x^26 + (406*a +
202)*x^25 + (4*a - 116)*x^24 + (-429*a + 131)*x^23 + (160*a -
105)*x^22 + (-2*a - 427)*x^21 + (-268*a - 220)*x^20 + (-5*a -
79)*x^19 + (-400*a - 211)*x^18 + (105*a + 129)*x^17 + (365*a +
82)*x^16 + (-76*a - 384)*x^15 + (-277*a - 395)*x^14 + (92*a -
66)*x^13 + (-217*a - 161)*x^12 + (83*a - 181)*x^11 + (-272*a -
208)*x^10 + (-226*a + 245)*x^9 + (357*a + 98)*x^8 + (239*a +
236)*x^7 + (-396*a - 27)*x^6 + (-23*a - 365)*x^5 + (-363*a +
136)*x^4 + (-28*a - 54)*x^3 + (-344*a + 416)*x^2 + (141*a + 132)*x +
(21*a - 422)),
 (x^39*y + (-254*a + 303)*x^38*y + (204*a - 200)*x^37*y + (381*a +
363)*x^36*y + (275*a - 293)*x^35*y + (200*a - 267)*x^34*y + (-247*a
+ 282)*x^33*y + (397*a - 31)*x^32*y + (-124*a + 306)*x^31*y + (348*a
- 430)*x^30*y + (-58*a + 403)*x^29*y + (75*a + 244)*x^28*y + (47*a +
267)*x^27*y + (-193*a - 183)*x^26*y + (208*a + 271)*x^25*y + (-333*a
+ 90)*x^24*y + (139*a + 210)*x^23*y + (76*a - 314)*x^22*y + (-123*a
- 331)*x^21*y + (295*a + 75)*x^20*y + (29*a - 362)*x^19*y + (388*a -
304)*x^18*y + (-427*a - 321)*x^17*y + (40*a + 75)*x^16*y + (-155*a -
164)*x^15*y + (178*a + 306)*x^14*y + (12*a - 337)*x^13*y + (-328*a +
428)*x^12*y + (18*a - 401)*x^11*y + (-180*a - 32)*x^10*y + (-275*a -
358)*x^9*y + (247*a + 346)*x^8*y + (77*a + 235)*x^7*y + (-226*a +
111)*x^6*y + (153*a - 405)*x^5*y + (217*a - 157)*x^4*y + (122*a +
15)*x^3*y + (157*a + 161)*x^2*y + (252*a - 393)*x*y + (376*a +
228)*y)/(x^39 + (-254*a + 303)*x^38 + (351*a + 343)*x^37 + (194*a -
236)*x^36 + (426*a + 55)*x^35 + (-319*a + 160)*x^34 + (125*a +
86)*x^33 + (-43*a + 423)*x^32 + (174*a - 343)*x^31 + (158*a +
74)*x^30 + (144*a + 35)*x^29 + (-413*a + 400)*x^28 + (140*a -
296)*x^27 + (-298*a - 94)*x^26 + (-352*a + 74)*x^25 + (-130*a -
151)*x^24 + (-182*a - 243)*x^23 + (308*a + 287)*x^22 + (111*a -
174)*x^21 + (231*a - 288)*x^20 + (104*a + 50)*x^19 + (243*a -
274)*x^18 + (-180*a + 78)*x^17 + (-220*a - 328)*x^16 + (-144*a +
167)*x^15 + (129*a + 29)*x^14 + (346*a - 264)*x^13 + (385*a +
18)*x^12 + (202*a - 21)*x^11 + (-267*a + 352)*x^10 + (-139*a -
235)*x^9 + (45*a + 183)*x^8 + (-391*a - 329)*x^7 + (408*a + 344)*x^6
+ (-102*a + 278)*x^5 + (-265*a - 257)*x^4 + (125*a + 199)*x^3 +
(-292*a - 386)*x^2 + (-126*a + 211)*x + (-407*a + 344)))
```

3 hash

```
m = 'isogeny'                                                    ####### message m
h = hex_to_bin(hashlib.md5(m + J2 + J3).hexdigest()) ; h ; len(h) ####### Hash h  h = H(m,j_2,1 ... , j_2,t , j_3,1 ... , j_3,t
```

```
)
```

```
'10111011000010000110000101101111110010000010100011000111001101000000
00111010100010001110010000000011110100001100011010011101011110'
128
```

4 z_1 , … z_t

all z_i : b_i =1 -> (j_2,i, Φ_i , j_3,i) output

```
z = ['index']              ###########  z_i = z[i]

global psi_i_2_prime
for i in range(1,t+1):

    if h[i-1] == '0' :     ########  b_i = 0
        z.append(alpha[i]) #######   z_i = α_i


    else:
        psi_i_2_prime=EllipticCurveIsogeny(E2[i], psi[i](P1))
########  b_i = 1
        z.append((j2[i],EllipticCurveIsogeny(E2[i], psi[i](P1)),psi_i_2_prime.codomain().j_invariant()))          ########
E_2,i , kernel Ψ_i(P1)  --> Φ_i, j_3,i







for i in range(1,t+1):
    print( 'z_{} = {}'.format(i,z[i]))
```

```
WARNING: Output truncated!
full_output.txt
```

```
z_1 = (515*a + 716, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (285*a+129)*x + (507*a+262) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (713*a+733)*x +
(70*a+235) over Finite Field in a of size 863^2, 232*a + 541)
z_2 = 5
z_3 = (473*a + 144, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (156*a+400)*x + (395*a+233) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (566*a+536)*x +
(566*a+723) over Finite Field in a of size 863^2, 657*a + 665)
z_4 = (451*a + 551, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (128*a+738)*x + (528*a+725) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (383*a+296)*x +
(792*a+719) over Finite Field in a of size 863^2, 590*a + 114)
z_5 = (419*a + 148, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x +
(454*a+255) over Finite Field in a of size 863^2, 89)
z_6 = 12
z_7 = (633*a + 848, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (268*a+786)*x +
(563*a+138) over Finite Field in a of size 863^2, 494)
z_8 = (230*a + 618, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (580*a+353)*x +
(76*a+790) over Finite Field in a of size 863^2, 633*a + 848)
z_9 = 25
z_10 = 13
z_11 = 0
z_12 = 19
z_13 = (281*a + 827, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (741*a+520)*x + (603*a+610) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(59*a+483)*x + (212*a+305) over Finite Field in a of size 863^2,
451*a + 551)
z_14 = 24
z_15 = 27
z_16 = 17
z_17 = 27
z_18 = (390*a + 617, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (707*a+556)*x + (468*a+628) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(209*a+216)*x + (142*a+433) over Finite Field in a of size 863^2,
406*a + 197)
z_19 = (343*a + 634, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (501*a+615)*x + (587*a+427) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(551*a+484)*x + (778*a+382) over Finite Field in a of size 863^2,
```

```
406*a + 197)
z_20 = 19
z_21 = 7
z_22 = 7
z_23 = 3
z_24 = (696, Isogeny of degree 16 from Elliptic Curve defined by y^2
= x^3 + 242*x + 608 over Finite Field in a of size 863^2 to Elliptic
Curve defined by y^2 = x^3 + (632*a+237)*x + (53*a+712) over Finite
Field in a of size 863^2, 482)
z_25 = 9
z_26 = (281*a + 827, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (741*a+520)*x + (603*a+610) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(59*a+483)*x + (212*a+305) over Finite Field in a of size 863^2,
451*a + 551)
z_27 = (473*a + 144, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (156*a+400)*x + (395*a+233) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(566*a+536)*x + (566*a+723) over Finite Field in a of size 863^2,
657*a + 665)
z_28 = 22
z_29 = (473*a + 144, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (156*a+400)*x + (468*a+630) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(456*a+133)*x + (29*a+65) over Finite Field in a of size 863^2,
657*a + 665)
z_30 = (696, Isogeny of degree 16 from Elliptic Curve defined by y^2
= x^3 + 242*x + 608 over Finite Field in a of size 863^2 to Elliptic
Curve defined by y^2 = x^3 + (632*a+237)*x + (53*a+712) over Finite
Field in a of size 863^2, 482)
z_31 = (257, Isogeny of degree 16 from Elliptic Curve defined by y^2
= x^3 + (690*a+584)*x + (227*a+410) over Finite Field in a of size
863^2 to Elliptic Curve defined by y^2 = x^3 + (766*a+480)*x +
(453*a+761) over Finite Field in a of size 863^2, 232*a + 541)
z_32 = (348*a + 368, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(768*a+443)*x + (782*a+752) over Finite Field in a of size 863^2,
803*a + 599)
z_33 = (348*a + 368, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(768*a+443)*x + (782*a+752) over Finite Field in a of size 863^2,
803*a + 599)
z_34 = (444*a + 567, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (389*a+152)*x + (383*a+717) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(336*a+306)*x + (852*a+126) over Finite Field in a of size 863^2,
22)
z_35 = 8
z_36 = 0
z_37 = (390*a + 617, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (707*a+556)*x + (395*a+235) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(769*a+127)*x + (483*a+583) over Finite Field in a of size 863^2,
527*a + 557)
z_38 = 16
z_39 = 14
z_40 = 12
z_41 = 15
z_42 = 8
z_43 = (419*a + 148, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (383*a+626) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(11*a+341)*x + (854*a+259) over Finite Field in a of size 863^2,
509*a + 781)
z_44 = 11
z_45 = (412*a + 139, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (735*a+3)*x + (528*a+473) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(846*a+213)*x + (279*a+135) over Finite Field in a of size 863^2,
527*a + 557)
z_46 = 11
z_47 = 25
z_48 = 16
z_49 = (241, Isogeny of degree 16 from Elliptic Curve defined by y^2
= x^3 + 649*x + (594*a+566) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (474*a+642)*x + (89*a+114)
over Finite Field in a of size 863^2, 803*a + 599)
z_50 = (419*a + 148, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2,
89)
z_51 = 17
z_52 = 19
z_53 = 11
```

```
z_54 = (696, Isogeny of degree 16 from Elliptic Curve defined by y^2
= x^3 + 242*x + 255 over Finite Field in a of size 863^2 to Elliptic
Curve defined by y^2 = x^3 + (710*a+204)*x + (814*a+648) over Finite
Field in a of size 863^2, 853*a + 60)
z_55 = (582*a + 245, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (122*a+398)*x + (603*a+513) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(220*a+564)*x + (163*a+371) over Finite Field in a of size 863^2,
509*a + 781)
z_56 = (515*a + 716, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (285*a+129)*x + (507*a+262) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(713*a+733)*x + (70*a+235) over Finite Field in a of size 863^2,
232*a + 541)
z_57 = 4
z_58 = 26
z_59 = (241, Isogeny of degree 16 from Elliptic Curve defined by y^2
= x^3 + 649*x + (594*a+566) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (474*a+642)*x + (89*a+114)
over Finite Field in a of size 863^2, 803*a + 599)

...

z_69 = 12
z_70 = (419*a + 148, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2,
89)
z_71 = (348*a + 368, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(768*a+443)*x + (782*a+752) over Finite Field in a of size 863^2,
803*a + 599)
z_72 = (520*a + 114, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (362*a+253)*x + (587*a+712) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(42*a+735)*x + (103*a+540) over Finite Field in a of size 863^2,
250*a + 693)
z_73 = 15
z_74 = (515*a + 716, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (285*a+129)*x + (356*a+601) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(686*a+292)*x + (679*a+591) over Finite Field in a of size 863^2,
548*a + 32)
z_75 = 18
z_76 = (230*a + 618, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(580*a+353)*x + (76*a+790) over Finite Field in a of size 863^2,
633*a + 848)
z_77 = 3
z_78 = 19
z_79 = 15
z_80 = (343*a + 634, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (501*a+615)*x + (587*a+427) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(551*a+484)*x + (778*a+382) over Finite Field in a of size 863^2,
406*a + 197)
z_81 = 23
z_82 = 13
z_83 = 13
z_84 = (241, Isogeny of degree 16 from Elliptic Curve defined by y^2
= x^3 + 649*x + (594*a+566) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (474*a+642)*x + (89*a+114)
over Finite Field in a of size 863^2, 803*a + 599)
z_85 = (633*a + 848, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2,
494)
z_86 = (412*a + 139, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (735*a+3)*x + (335*a+390) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(467*a+299)*x + (409*a+790) over Finite Field in a of size 863^2,
740*a + 293)
z_87 = 4
z_88 = 15
z_89 = (473*a + 144, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (156*a+400)*x + (468*a+630) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(456*a+133)*x + (29*a+65) over Finite Field in a of size 863^2,
657*a + 665)
z_90 = 20
z_91 = 3
z_92 = 12
z_93 = 13
```

```
z_94 = 10
z_95 = 19
z_96 = 18
z_97 = 10
z_98 = (419*a + 148, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2,
89)
z_99 = (390*a + 617, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (707*a+556)*x + (468*a+628) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(209*a+216)*x + (142*a+433) over Finite Field in a of size 863^2,
406*a + 197)
z_100 = (419*a + 148, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (383*a+626) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(11*a+341)*x + (854*a+259) over Finite Field in a of size 863^2,
509*a + 781)
z_101 = (343*a + 634, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (501*a+615)*x + (587*a+427) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(551*a+484)*x + (778*a+382) over Finite Field in a of size 863^2,
406*a + 197)
z_102 = 5
z_103 = (473*a + 144, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (156*a+400)*x + (395*a+233) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(566*a+536)*x + (566*a+723) over Finite Field in a of size 863^2,
657*a + 665)
z_104 = 11
z_105 = 13
z_106 = 13
z_107 = 24
z_108 = (582*a + 245, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (122*a+398)*x + (603*a+513) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(220*a+564)*x + (163*a+371) over Finite Field in a of size 863^2,
509*a + 781)
z_109 = (343*a + 634, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (501*a+615)*x + (587*a+427) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(551*a+484)*x + (778*a+382) over Finite Field in a of size 863^2,
406*a + 197)
z_110 = 14
z_111 = 8
z_112 = 13
z_113 = (633*a + 848, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2,
494)
z_114 = (230*a + 618, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(580*a+353)*x + (76*a+790) over Finite Field in a of size 863^2,
633*a + 848)
z_115 = 3
z_116 = (348*a + 368, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (578*a+414)*x + (507*a+94) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(89*a+584)*x + (75*a+76) over Finite Field in a of size 863^2, 152*a
+ 605)
z_117 = 18
z_118 = 3
z_119 = (390*a + 617, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (707*a+556)*x + (395*a+235) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(769*a+127)*x + (483*a+583) over Finite Field in a of size 863^2,
527*a + 557)
z_120 = (633*a + 848, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2,
494)
z_121 = (473*a + 144, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (156*a+400)*x + (468*a+630) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(456*a+133)*x + (29*a+65) over Finite Field in a of size 863^2,
657*a + 665)
z_122 = 25
z_123 = (348*a + 368, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(768*a+443)*x + (782*a+752) over Finite Field in a of size 863^2,
803*a + 599)
z_124 = 11
```

```
z_125 = (412*a + 139, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (735*a+3)*x + (335*a+390) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(467*a+299)*x + (409*a+790) over Finite Field in a of size 863^2,
740*a + 293)
z_126 = (419*a + 148, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2,
89)
z_127 = (419*a + 148, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (383*a+626) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(11*a+341)*x + (854*a+259) over Finite Field in a of size 863^2,
509*a + 781)
z_128 = 6
```

full_output.txt

example) j_2,2 , Φ_2, j_3,2 check

```
z[1]
```

```
(515*a + 716,
 Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(285*a+129)*x + (507*a+262) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (713*a+733)*x + (70*a+235)
over Finite Field in a of size 863^2,
 232*a + 541)
```

```
z[2]  ### ( j_2,2 , Φ_2 , j_3,2 )
```

```
5
```

```
z[3]
```

```
(473*a + 144,
 Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(156*a+400)*x + (395*a+233) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (566*a+536)*x + (566*a+723)
over Finite Field in a of size 863^2,
 657*a + 665)
```

```
psi[1].rational_maps()
```

```
((x^27 + (-289*a + 176)*x^26 + (342*a + 412)*x^25 + (-46*a +
351)*x^24 + (208*a - 126)*x^23 + (-274*a - 306)*x^22 + (137*a -
261)*x^21 + (-174*a - 35)*x^20 + (54*a + 103)*x^19 + (-347*a -
255)*x^18 + (286*a - 366)*x^17 + (389*a + 157)*x^16 + (425*a +
388)*x^15 + (285*a - 285)*x^14 + (270*a - 184)*x^13 + (374*a -
78)*x^12 + (-37*a + 337)*x^11 + (-274*a - 230)*x^10 + (302*a -
156)*x^9 + (-90*a - 209)*x^8 + (124*a + 133)*x^7 + (-108*a - 7)*x^6
+ (-133*a - 386)*x^5 + (-340*a + 159)*x^4 + (55*a + 262)*x^3 +
(111*a + 10)*x^2 + (79*a + 58)*x + (-111*a + 420))/(x^26 + (-289*a +
176)*x^25 + (399*a + 265)*x^24 + (69*a + 170)*x^23 + (392*a -
15)*x^22 + (-296*a + 195)*x^21 + (-202*a + 151)*x^20 + (52*a +
39)*x^19 + (145*a + 406)*x^18 + (360*a - 103)*x^17 + (-52*a +
197)*x^16 + (-35*a + 421)*x^15 + (58*a + 126)*x^14 + (-265*a +
127)*x^13 + (-190*a - 378)*x^12 + (-116*a + 142)*x^11 + (-212*a +
67)*x^10 + (-298*a - 396)*x^9 + (-265*a - 254)*x^8 + (420*a +
269)*x^7 + (-347*a - 290)*x^6 + (-362*a + 73)*x^5 + (-387*a -
74)*x^4 + (412*a + 246)*x^3 + (-74*a - 67)*x^2 + (-221*a + 238)*x +
(23*a - 190)),
 (x^39*y + (-2*a + 264)*x^38*y + (-239*a - 75)*x^37*y + (-78*a -
350)*x^36*y + (112*a - 290)*x^35*y + (-334*a - 202)*x^34*y + (-345*a
- 220)*x^33*y + (422*a + 197)*x^32*y + (276*a + 336)*x^31*y + (71*a
- 313)*x^30*y + (-431*a - 197)*x^29*y + (76*a - 29)*x^28*y + (-428*a
- 59)*x^27*y + (-216*a + 30)*x^26*y + (261*a + 121)*x^25*y + (422*a
+ 169)*x^24*y + (98*a - 230)*x^23*y + (236*a + 180)*x^22*y + (-294*a
- 315)*x^21*y + (269*a - 11)*x^20*y + (-66*a + 30)*x^19*y + (-88*a +
412)*x^18*y + (83*a - 100)*x^17*y + (240*a - 204)*x^16*y + (-85*a -
308)*x^15*y + (-226*a - 341)*x^14*y + (-267*a + 328)*x^13*y +
(-408*a + 206)*x^12*y + (332*a - 153)*x^11*y + (358*a + 403)*x^10*y
+ (140*a - 354)*x^9*y + (-324*a - 368)*x^8*y + (237*a - 80)*x^7*y +
(361*a + 129)*x^6*y + (170*a + 267)*x^5*y + (136*a + 323)*x^4*y +
(-219*a - 265)*x^3*y + (-158*a - 224)*x^2*y + (-30*a - 184)*x*y +
(-343*a + 204)*y)/(x^39 + (-2*a + 264)*x^38 + (-296*a + 72)*x^37 +
(-410*a + 211)*x^36 + (-395*a + 62)*x^35 + (380*a - 69)*x^34 +
(424*a - 373)*x^33 + (211*a + 400)*x^32 + (-369*a - 267)*x^31 +
(230*a - 221)*x^30 + (-74*a + 348)*x^29 + (-272*a + 161)*x^28 +
(14*a + 25)*x^27 + (86*a + 97)*x^26 + (286*a - 316)*x^25 + (137*a -
52)*x^24 + (265*a + 254)*x^23 + (-369*a + 337)*x^22 + (112*a -
204)*x^21 + (-189*a + 246)*x^20 + (-198*a + 330)*x^19 + (-346*a +
414)*x^18 + (-18*a + 293)*x^17 + (351*a - 73)*x^16 + (-9*a -
380)*x^15 + (-186*a - 225)*x^14 + (-45*a - 401)*x^13 + (-2*a +
384)*x^12 + (406*a + 104)*x^11 + (-31*a - 363)*x^10 + (86*a +
43)*x^9 + (235*a - 50)*x^8 + (-31*a - 371)*x^7 + (355*a + 234)*x^6 +
(-430*a - 212)*x^5 + (-178*a - 271)*x^4 + (151*a - 184)*x^3 + (16*a
- 53)*x^2 + (50*a - 169)*x + (-174*a - 78)))
```

```
psi[3].rational_maps()
```

```
((x^27 + (-395*a - 351)*x^26 + (-413*a + 135)*x^25 + (240*a -
336)*x^24 + (10*a - 317)*x^23 + (-303*a - 123)*x^22 + (-112*a -
218)*x^21 + (-138*a - 283)*x^20 + (-301*a - 314)*x^19 + (-89*a +
165)*x^18 + (5*a - 69)*x^17 + (356*a - 374)*x^16 + (-18*a - 71)*x^15
+ (405*a + 133)*x^14 + (303*a + 275)*x^13 + (382*a - 392)*x^12 +
(-161*a - 235)*x^11 + (-21*a - 107)*x^10 + (-394*a + 343)*x^9 +
(207*a + 144)*x^8 + (-328*a + 328)*x^7 + (357*a - 53)*x^6 + (404*a +
205)*x^5 + (171*a - 150)*x^4 + (132*a - 270)*x^3 + (-22*a + 83)*x^2
+ (-319*a - 356)*x + (282*a - 117))/(x^26 + (-395*a - 351)*x^25 +
(136*a - 303)*x^24 + (-402*a + 45)*x^23 + (130*a + 8)*x^22 + (-202*a
+ 146)*x^21 + (-389*a + 239)*x^20 + (197*a - 289)*x^19 + (363*a +
358)*x^18 + (94*a - 354)*x^17 + (146*a - 55)*x^16 + (358*a -
406)*x^15 + (174*a - 349)*x^14 + (403*a + 373)*x^13 + (-198*a -
240)*x^12 + (-302*a - 359)*x^11 + (-295*a + 75)*x^10 + (-358*a -
112)*x^9 + (-351*a + 94)*x^8 + (76*a - 135)*x^7 + (129*a - 17)*x^6 +
(311*a - 269)*x^5 + (357*a + 328)*x^4 + (-298*a - 139)*x^3 + (71*a -
355)*x^2 + (-216*a + 175)*x + (-74*a - 92)),
 (x^39*y + (-161*a - 95)*x^38*y + (247*a - 421)*x^37*y + (234*a +
293)*x^36*y + (61*a + 178)*x^35*y + (-166*a - 355)*x^34*y + (-48*a +
386)*x^33*y + (-10*a + 191)*x^32*y + (-22*a - 227)*x^31*y + (408*a -
181)*x^30*y + (171*a + 304)*x^29*y + (-327*a + 142)*x^28*y + (176*a
+ 76)*x^27*y + (-314*a - 256)*x^26*y + (-200*a + 294)*x^25*y + (32*a
+ 431)*x^24*y + (185*a + 343)*x^23*y + (-232*a + 300)*x^22*y + (62*a
- 284)*x^21*y + (109*a - 183)*x^20*y + (-128*a + 426)*x^19*y + (-a +
212)*x^18*y + (-210*a + 121)*x^17*y + (-271*a - 89)*x^16*y + (392*a
+ 222)*x^15*y + (25*a - 153)*x^14*y + (-15*a + 95)*x^13*y + (72*a +
256)*x^12*y + (248*a + 101)*x^11*y + (-124*a + 53)*x^10*y + (204*a -
132)*x^9*y + (140*a - 190)*x^8*y + (-215*a + 218)*x^7*y + (264*a +
375)*x^6*y + (-287*a - 112)*x^5*y + (-88*a + 102)*x^4*y + (35*a -
221)*x^3*y + (-415*a + 418)*x^2*y + (425*a - 187)*x*y + (-144*a +
270)*y)/(x^39 + (-161*a - 95)*x^38 + (-302*a + 17)*x^37 + (-249*a +
198)*x^36 + (-89*a - 252)*x^35 + (-34*a - 17)*x^34 + (-286*a -
237)*x^33 + (-135*a - 244)*x^32 + (-421*a - 329)*x^31 + (-312*a +
287)*x^30 + (-229*a - 248)*x^29 + (-156*a - 290)*x^28 + (-228*a -
131)*x^27 + (228*a + 358)*x^26 + (-254*a + 36)*x^25 + (a - 108)*x^24
+ (-363*a - 126)*x^23 + (138*a + 69)*x^22 + (111*a + 400)*x^21 +
(-170*a - 384)*x^20 + (431*a + 30)*x^19 + (7*a - 423)*x^18 + (17*a +
62)*x^17 + (159*a - 263)*x^16 + (-415*a - 32)*x^15 + (-83*a +
219)*x^14 + (-119*a + 359)*x^13 + (-175*a - 370)*x^12 + (298*a +
172)*x^11 + (393*a + 115)*x^10 + (236*a - 430)*x^9 + (271*a +
217)*x^8 + (371*a - 123)*x^7 + (156*a + 255)*x^6 + (-228*a - 76)*x^5
+ (396*a - 123)*x^4 + (294*a - 287)*x^3 + (328*a + 37)*x^2 + (267*a
+ 128)*x + (-176*a + 290)))
```

5 signature

```
signature = (( h , z) , m) ;print('₩n'); print(signature)    ##### signature = (h , z_1,z_2 ... z_t ) , m
```

```
(('10111011000010000110000101101111110010000010100011000111001101000₩
0000111010100010001110010000000011110100001100011010011101011110',
['index', (515*a + 716, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (285*a+129)*x + (507*a+262) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(713*a+733)*x + (70*a+235) over Finite Field in a of size 863^2,
232*a + 541), 5, (473*a + 144, Isogeny of degree 16 from Elliptic
Curve defined by y^2 = x^3 + (156*a+400)*x + (395*a+233) over Finite
Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(566*a+536)*x + (566*a+723) over Finite Field in a of size 863^2,
657*a + 665), (451*a + 551, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (128*a+738)*x + (528*a+725) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(383*a+296)*x + (792*a+719) over Finite Field in a of size 863^2,
590*a + 114), (419*a + 148, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2,
89), 12, (633*a + 848, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2,
494), (230*a + 618, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (580*a+353)*x +
(76*a+790) over Finite Field in a of size 863^2, 633*a + 848), 25,
13, 0, 19, (281*a + 827, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (741*a+520)*x + (603*a+610) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(59*a+483)*x + (212*a+305) over Finite Field in a of size 863^2,
451*a + 551), 24, 27, 17, 27, (390*a + 617, Isogeny of degree 16
from Elliptic Curve defined by y^2 = x^3 + (707*a+556)*x +
(468*a+628) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (209*a+216)*x + (142*a+433) over Finite Field
in a of size 863^2, 406*a + 197), (343*a + 634, Isogeny of degree 16
from Elliptic Curve defined by y^2 = x^3 + (501*a+615)*x +
```

```
(587*a+427) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (551*a+484)*x + (778*a+382) over Finite Field
in a of size 863^2, 406*a + 197), 19, 7, 7, 3, (696, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + 242*x + 608
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (632*a+237)*x + (53*a+712) over Finite Field in a of
size 863^2, 482), 9, (281*a + 827, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (741*a+520)*x + (603*a+610)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (59*a+483)*x + (212*a+305) over Finite Field in a of
size 863^2, 451*a + 551), (473*a + 144, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (156*a+400)*x + (395*a+233)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (566*a+536)*x + (566*a+723) over Finite Field in a of
size 863^2, 657*a + 665), 22, (473*a + 144, Isogeny of degree 16
from Elliptic Curve defined by y^2 = x^3 + (156*a+400)*x +
(468*a+630) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (456*a+133)*x + (29*a+65) over Finite Field
in a of size 863^2, 657*a + 665), (696, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + 242*x + 608 over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(632*a+237)*x + (53*a+712) over Finite Field in a of size 863^2,
482), (257, Isogeny of degree 16 from Elliptic Curve defined by y^2
= x^3 + (690*a+584)*x + (227*a+410) over Finite Field in a of size
863^2 to Elliptic Curve defined by y^2 = x^3 + (766*a+480)*x +
(453*a+761) over Finite Field in a of size 863^2, 232*a + 541),
(348*a + 368, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (768*a+443)*x +
(782*a+752) over Finite Field in a of size 863^2, 803*a + 599),
(348*a + 368, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (768*a+443)*x +
(782*a+752) over Finite Field in a of size 863^2, 803*a + 599),
(444*a + 567, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (389*a+152)*x + (383*a+717) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (336*a+306)*x +
(852*a+126) over Finite Field in a of size 863^2, 22), 8, 0, (390*a
+ 617, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3
+ (707*a+556)*x + (395*a+235) over Finite Field in a of size 863^2
to Elliptic Curve defined by y^2 = x^3 + (769*a+127)*x + (483*a+583)
over Finite Field in a of size 863^2, 527*a + 557), 16, 14, 12, 15,
8, (419*a + 148, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (474*a+541)*x + (383*a+626) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (11*a+341)*x +
(854*a+259) over Finite Field in a of size 863^2, 509*a + 781), 11,
(412*a + 139, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (735*a+3)*x + (528*a+473) over Finite Field in a of size
863^2 to Elliptic Curve defined by y^2 = x^3 + (846*a+213)*x +
(279*a+135) over Finite Field in a of size 863^2, 527*a + 557), 11,
25, 16, (241, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + 649*x + (594*a+566) over Finite Field in a of size 863^2
to Elliptic Curve defined by y^2 = x^3 + (474*a+642)*x + (89*a+114)
over Finite Field in a of size 863^2, 803*a + 599), (419*a + 148,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(474*a+541)*x + (480*a+237) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x + (454*a+255)
over Finite Field in a of size 863^2, 89), 17, 19, 11, (696, Isogeny
of degree 16 from Elliptic Curve defined by y^2 = x^3 + 242*x + 255
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (710*a+204)*x + (814*a+648) over Finite Field in a of
size 863^2, 853*a + 60), (582*a + 245, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (122*a+398)*x + (603*a+513)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (220*a+564)*x + (163*a+371) over Finite Field in a of
size 863^2, 509*a + 781), (515*a + 716, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (285*a+129)*x + (507*a+262)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (713*a+733)*x + (70*a+235) over Finite Field in a of
size 863^2, 232*a + 541), 4, 26, (241, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + 649*x + (594*a+566) over
Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 =
x^3 + (474*a+642)*x + (89*a+114) over Finite Field in a of size
863^2, 803*a + 599), (390*a + 617, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (707*a+556)*x + (395*a+235)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (769*a+127)*x + (483*a+583) over Finite Field in a of
size 863^2, 527*a + 557), 0, (451*a + 551, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (128*a+738)*x + (335*a+138)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (202*a+65)*x + (645*a+721) over Finite Field in a of
size 863^2, 371*a + 206), 21, 19, 6, 2, 4, 15, 12, (419*a + 148,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(474*a+541)*x + (480*a+237) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x + (454*a+255)
over Finite Field in a of size 863^2, 89), (348*a + 368, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + (578*a+414)*x +
```

```
(356*a+769) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (768*a+443)*x + (782*a+752) over Finite Field
in a of size 863^2, 803*a + 599), (520*a + 114, Isogeny of degree 16
from Elliptic Curve defined by y^2 = x^3 + (362*a+253)*x +
(587*a+712) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (42*a+735)*x + (103*a+540) over Finite Field
in a of size 863^2, 250*a + 693), 15, (515*a + 716, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + (285*a+129)*x +
(356*a+601) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (686*a+292)*x + (679*a+591) over Finite Field
in a of size 863^2, 548*a + 32), 18, (230*a + 618, Isogeny of degree
16 from Elliptic Curve defined by y^2 = x^3 + (390*a+301)*x +
(796*a+657) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (580*a+353)*x + (76*a+790) over Finite Field
in a of size 863^2, 633*a + 848), 3, 19, 15, (343*a + 634, Isogeny
of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(501*a+615)*x + (587*a+427) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (551*a+484)*x + (778*a+382)
over Finite Field in a of size 863^2, 406*a + 197), 23, 13, 13,
(241, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3
+ 649*x + (594*a+566) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (474*a+642)*x + (89*a+114)
over Finite Field in a of size 863^2, 803*a + 599), (633*a + 848,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(473*a+691)*x + (796*a+273) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (268*a+786)*x + (563*a+138)
over Finite Field in a of size 863^2, 494), (412*a + 139, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + (735*a+3)*x +
(335*a+390) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (467*a+299)*x + (409*a+790) over Finite Field
in a of size 863^2, 740*a + 293), 4, 15, (473*a + 144, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + (156*a+400)*x +
(468*a+630) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (456*a+133)*x + (29*a+65) over Finite Field
in a of size 863^2, 657*a + 665), 20, 3, 12, 13, 10, 19, 18, 10,
(419*a + 148, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x +
(454*a+255) over Finite Field in a of size 863^2, 89), (390*a + 617,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(707*a+556)*x + (468*a+628) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (209*a+216)*x + (142*a+433)
over Finite Field in a of size 863^2, 406*a + 197), (419*a + 148,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(474*a+541)*x + (383*a+626) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (11*a+341)*x + (854*a+259)
over Finite Field in a of size 863^2, 509*a + 781), (343*a + 634,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(501*a+615)*x + (587*a+427) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (551*a+484)*x + (778*a+382)
over Finite Field in a of size 863^2, 406*a + 197), 5, (473*a + 144,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(156*a+400)*x + (395*a+233) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (566*a+536)*x + (566*a+723)
over Finite Field in a of size 863^2, 657*a + 665), 11, 13, 13, 24,
(582*a + 245, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (122*a+398)*x + (603*a+513) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (220*a+564)*x +
(163*a+371) over Finite Field in a of size 863^2, 509*a + 781),
(343*a + 634, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (501*a+615)*x + (587*a+427) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (551*a+484)*x +
(778*a+382) over Finite Field in a of size 863^2, 406*a + 197), 14,
8, 13, (633*a + 848, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2,
494), (230*a + 618, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (580*a+353)*x +
(76*a+790) over Finite Field in a of size 863^2, 633*a + 848), 3,
(348*a + 368, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (578*a+414)*x + (507*a+94) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (89*a+584)*x +
(75*a+76) over Finite Field in a of size 863^2, 152*a + 605), 18, 3,
(390*a + 617, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (707*a+556)*x + (395*a+235) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (769*a+127)*x +
(483*a+583) over Finite Field in a of size 863^2, 527*a + 557),
(633*a + 848, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (268*a+786)*x +
(563*a+138) over Finite Field in a of size 863^2, 494), (473*a +
144, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(156*a+400)*x + (468*a+630) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (456*a+133)*x + (29*a+65) over
Finite Field in a of size 863^2, 657*a + 665), 25, (348*a + 368,
```

```
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(578*a+414)*x + (356*a+769) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (768*a+443)*x + (782*a+752)
over Finite Field in a of size 863^2, 803*a + 599), 11, (412*a +
139, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(735*a+3)*x + (335*a+390) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (467*a+299)*x + (409*a+790)
over Finite Field in a of size 863^2, 740*a + 293), (419*a + 148,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(474*a+541)*x + (480*a+237) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x + (454*a+255)
over Finite Field in a of size 863^2, 89), (419*a + 148, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + (474*a+541)*x +
(383*a+626) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (11*a+341)*x + (854*a+259) over Finite Field
in a of size 863^2, 509*a + 781), 6]), 'isogeny')
```

<Verify>

```
print('m = {} Wnh = {} Wnz = {}'.format(m,h,z))          ## verify information
```

```
m = isogeny
h =
10111011000010000110000101101111110010000010100011000111001101000000W
01110101000100011100100000000111101000011000110100111010110
z = ['index', (515*a + 716, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (285*a+129)*x + (507*a+262) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(713*a+733)*x + (70*a+235) over Finite Field in a of size 863^2,
232*a + 541), 5, (473*a + 144, Isogeny of degree 16 from Elliptic
Curve defined by y^2 = x^3 + (156*a+400)*x + (395*a+233) over Finite
Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(566*a+536)*x + (566*a+723) over Finite Field in a of size 863^2,
657*a + 665), (451*a + 551, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (128*a+738)*x + (528*a+725) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(383*a+296)*x + (792*a+719) over Finite Field in a of size 863^2,
590*a + 114), (419*a + 148, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2,
89), 12, (633*a + 848, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2,
494), (230*a + 618, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (580*a+353)*x +
(76*a+790) over Finite Field in a of size 863^2, 633*a + 848), 25,
13, 0, 19, (281*a + 827, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (741*a+520)*x + (603*a+610) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(59*a+483)*x + (212*a+305) over Finite Field in a of size 863^2,
451*a + 551), 24, 27, 17, 27, (390*a + 617, Isogeny of degree 16
from Elliptic Curve defined by y^2 = x^3 + (707*a+556)*x +
(468*a+628) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (209*a+216)*x + (142*a+433) over Finite Field
in a of size 863^2, 406*a + 197), (343*a + 634, Isogeny of degree 16
from Elliptic Curve defined by y^2 = x^3 + (501*a+615)*x +
(587*a+427) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (551*a+484)*x + (778*a+382) over Finite Field
in a of size 863^2, 406*a + 197), 19, 7, 7, 3, (696, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + 242*x + 608
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (632*a+237)*x + (53*a+712) over Finite Field in a of
size 863^2, 482), 9, (281*a + 827, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (741*a+520)*x + (603*a+610)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (59*a+483)*x + (212*a+305) over Finite Field in a of
size 863^2, 451*a + 551), (473*a + 144, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (156*a+400)*x + (395*a+233)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (566*a+536)*x + (566*a+723) over Finite Field in a of
size 863^2, 657*a + 665), 22, (473*a + 144, Isogeny of degree 16
from Elliptic Curve defined by y^2 = x^3 + (156*a+400)*x +
(468*a+630) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (456*a+133)*x + (29*a+65) over Finite Field
in a of size 863^2, 657*a + 665), (696, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + 242*x + 608 over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(632*a+237)*x + (53*a+712) over Finite Field in a of size 863^2,
482), (257, Isogeny of degree 16 from Elliptic Curve defined by y^2
= x^3 + (690*a+584)*x + (227*a+410) over Finite Field in a of size
863^2 to Elliptic Curve defined by y^2 = x^3 + (766*a+480)*x +
(453*a+761) over Finite Field in a of size 863^2, 232*a + 541),
(348*a + 368, Isogeny of degree 16 from Elliptic Curve defined by
```

```
y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (768*a+443)*x +
(782*a+752) over Finite Field in a of size 863^2, 803*a + 599),
(348*a + 368, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (768*a+443)*x +
(782*a+752) over Finite Field in a of size 863^2, 803*a + 599),
(444*a + 567, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (389*a+152)*x + (383*a+717) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (336*a+306)*x +
(852*a+126) over Finite Field in a of size 863^2, 22), 8, 0, (390*a
+ 617, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3
+ (707*a+556)*x + (395*a+235) over Finite Field in a of size 863^2
to Elliptic Curve defined by y^2 = x^3 + (769*a+127)*x + (483*a+583)
over Finite Field in a of size 863^2, 527*a + 557), 16, 14, 12, 15,
8, (419*a + 148, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (474*a+541)*x + (383*a+626) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (11*a+341)*x +
(854*a+259) over Finite Field in a of size 863^2, 509*a + 781), 11,
(412*a + 139, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (735*a+3)*x + (528*a+473) over Finite Field in a of size
863^2 to Elliptic Curve defined by y^2 = x^3 + (846*a+213)*x +
(279*a+135) over Finite Field in a of size 863^2, 527*a + 557), 11,
25, 16, (241, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + 649*x + (594*a+566) over Finite Field in a of size 863^2
to Elliptic Curve defined by y^2 = x^3 + (474*a+642)*x + (89*a+114)
over Finite Field in a of size 863^2, 803*a + 599), (419*a + 148,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(474*a+541)*x + (480*a+237) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x + (454*a+255)
over Finite Field in a of size 863^2, 89), 17, 19, 11, (696, Isogeny
of degree 16 from Elliptic Curve defined by y^2 = x^3 + 242*x + 255
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (710*a+204)*x + (814*a+648) over Finite Field in a of
size 863^2, 853*a + 60), (582*a + 245, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (122*a+398)*x + (603*a+513)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (220*a+564)*x + (163*a+371) over Finite Field in a of
size 863^2, 509*a + 781), (515*a + 716, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (285*a+129)*x + (507*a+262)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (713*a+733)*x + (70*a+235) over Finite Field in a of
size 863^2, 232*a + 541), 4, 26, (241, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + 649*x + (594*a+566) over
Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 =
x^3 + (474*a+642)*x + (89*a+114) over Finite Field in a of size
863^2, 803*a + 599), (390*a + 617, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (707*a+556)*x + (395*a+235)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (769*a+127)*x + (483*a+583) over Finite Field in a of
size 863^2, 527*a + 557), 0, (451*a + 551, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (128*a+738)*x + (335*a+138)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (202*a+65)*x + (645*a+721) over Finite Field in a of
size 863^2, 371*a + 206), 21, 19, 6, 2, 4, 15, 12, (419*a + 148,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(474*a+541)*x + (480*a+237) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x + (454*a+255)
over Finite Field in a of size 863^2, 89), (348*a + 368, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + (578*a+414)*x +
(356*a+769) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (768*a+443)*x + (782*a+752) over Finite Field
in a of size 863^2, 803*a + 599), (520*a + 114, Isogeny of degree 16
from Elliptic Curve defined by y^2 = x^3 + (362*a+253)*x +
(587*a+712) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (42*a+735)*x + (103*a+540) over Finite Field
in a of size 863^2, 250*a + 693), 15, (515*a + 716, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + (285*a+129)*x +
(356*a+601) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (686*a+292)*x + (679*a+591) over Finite Field
in a of size 863^2, 548*a + 32), 18, (230*a + 618, Isogeny of degree
16 from Elliptic Curve defined by y^2 = x^3 + (390*a+301)*x +
(796*a+657) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (580*a+353)*x + (76*a+790) over Finite Field
in a of size 863^2, 633*a + 848), 3, 19, 15, (343*a + 634, Isogeny
of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(501*a+615)*x + (587*a+427) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (551*a+484)*x + (778*a+382)
over Finite Field in a of size 863^2, 406*a + 197), 23, 13, 13,
(241, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3
+ 649*x + (594*a+566) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (474*a+642)*x + (89*a+114)
over Finite Field in a of size 863^2, 803*a + 599), (633*a + 848,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(473*a+691)*x + (796*a+273) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (268*a+786)*x + (563*a+138)
over Finite Field in a of size 863^2, 494), (412*a + 139, Isogeny of
```

```
degree 16 from Elliptic Curve defined by y^2 = x^3 + (735*a+3)*x +
(335*a+390) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (467*a+299)*x + (409*a+790) over Finite Field
in a of size 863^2, 740*a + 293), 4, 15, (473*a + 144, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + (156*a+400)*x +
(468*a+630) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (456*a+133)*x + (29*a+65) over Finite Field
in a of size 863^2, 657*a + 665), 20, 3, 12, 13, 10, 19, 18, 10,
(419*a + 148, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x +
(454*a+255) over Finite Field in a of size 863^2, 89), (390*a + 617,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(707*a+556)*x + (468*a+628) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (209*a+216)*x + (142*a+433)
over Finite Field in a of size 863^2, 406*a + 197), (419*a + 148,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(474*a+541)*x + (383*a+626) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (11*a+341)*x + (854*a+259)
over Finite Field in a of size 863^2, 509*a + 781), (343*a + 634,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(501*a+615)*x + (587*a+427) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (551*a+484)*x + (778*a+382)
over Finite Field in a of size 863^2, 406*a + 197), 5, (473*a + 144,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(156*a+400)*x + (395*a+233) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (566*a+536)*x + (566*a+723)
over Finite Field in a of size 863^2, 657*a + 665), 11, 13, 13, 24,
(582*a + 245, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (122*a+398)*x + (603*a+513) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (220*a+564)*x +
(163*a+371) over Finite Field in a of size 863^2, 509*a + 781),
(343*a + 634, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (501*a+615)*x + (587*a+427) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (551*a+484)*x +
(778*a+382) over Finite Field in a of size 863^2, 406*a + 197), 14,
8, 13, (633*a + 848, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2,
494), (230*a + 618, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (580*a+353)*x +
(76*a+790) over Finite Field in a of size 863^2, 633*a + 848), 3,
(348*a + 368, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (578*a+414)*x + (507*a+94) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (89*a+584)*x +
(75*a+76) over Finite Field in a of size 863^2, 152*a + 605), 18, 3,
(390*a + 617, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (707*a+556)*x + (395*a+235) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (769*a+127)*x +
(483*a+583) over Finite Field in a of size 863^2, 527*a + 557),
(633*a + 848, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (268*a+786)*x +
(563*a+138) over Finite Field in a of size 863^2, 494), (473*a +
144, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(156*a+400)*x + (468*a+630) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (456*a+133)*x + (29*a+65) over
Finite Field in a of size 863^2, 657*a + 665), 25, (348*a + 368,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(578*a+414)*x + (356*a+769) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (768*a+443)*x + (782*a+752)
over Finite Field in a of size 863^2, 803*a + 599), 11, (412*a +
139, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(735*a+3)*x + (335*a+390) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (467*a+299)*x + (409*a+790)
over Finite Field in a of size 863^2, 740*a + 293), (419*a + 148,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(474*a+541)*x + (480*a+237) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x + (454*a+255)
over Finite Field in a of size 863^2, 89), (419*a + 148, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + (474*a+541)*x +
(383*a+626) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (11*a+341)*x + (854*a+259) over Finite Field
in a of size 863^2, 509*a + 781), 6]
```

```
######################## signer : j_2,i  v.s  verifier : j_2,i
######################## signer : j_3,i  v.s  verifier : j_3,i

j2_verify = ['index']           ########## j2_verify[i] = verifier 의 j_2,i
j3_verify = ['index']           ########## j3_verify[i] = verifier 의 j_3,i

for i in range(1,t+1):

    if h[i-1] == '0' :                                                                  ###### b_i =
0  i.e, z_i = α_i  Case
```

```
        j2_verify.append(EllipticCurveIsogeny(E0, R2 + z[i]*S2).codomain().j_invariant())                    ###### domain
E0 , kernel R2 + [z_i]S2 --> using isogeny --> j_2,i
        j3_verify.append(EllipticCurveIsogeny(E1, R2_prime + z[i]*S2_prime).codomain().j_invariant())        ###### domain
E1 , kernel R'2 + [z_i]S'2 --> using isogeny --> j_3,i

    else:                                                                                                    ###### b_i = 1
i.e , z_i = j_2,i  Case
        j2_verify.append(z[i][0])                                                                            ###### j_2,i =
z_i
        j3_verify.append((psi_i_2_prime.codomain()).j_invariant())                  ###### domain E_2,i , kernel Ψ_i(P1) -->
isogeny --> j_3,i

J2_VERIFY = ''                  ########## J2_VERIFY = j_2,i all sequences
J3_VERIFY = ''                  ########## J3_VERIFY = j_3,i all sequences

for j2_ver in j2_verify[1:]:
    J2_VERIFY += str(j2_ver)
for j3_ver in j3_verify[1:]:
    J3_VERIFY += str(j3_ver)
```

```
for i in range(1,t+1):
    print("Verify 과정 j_2,{} = {} , j_3,{} = {} ₩nSign 때 계산한 j_2,{} = {} , j_3,{} =
{}₩n".format(i,j2_verify[i],i,j3_verify[i],i,j2[i],i,j3[i]))
```

WARNING: Output truncated!
full_output.txt

Verify 과정 j_2,1 = 515*a + 716 , j_3,1 = 232*a + 541
Sign 때 계산한 j_2,1 = 515*a + 716 , j_3,1 = 232*a + 541

Verify 과정 j_2,2 = 473*a + 144 , j_3,2 = 657*a + 665
Sign 때 계산한 j_2,2 = 473*a + 144 , j_3,2 = 657*a + 665

Verify 과정 j_2,3 = 473*a + 144 , j_3,3 = 657*a + 665
Sign 때 계산한 j_2,3 = 473*a + 144 , j_3,3 = 657*a + 665

Verify 과정 j_2,4 = 451*a + 551 , j_3,4 = 590*a + 114
Sign 때 계산한 j_2,4 = 451*a + 551 , j_3,4 = 590*a + 114

Verify 과정 j_2,5 = 419*a + 148 , j_3,5 = 89
Sign 때 계산한 j_2,5 = 419*a + 148 , j_3,5 = 89

Verify 과정 j_2,6 = 696 , j_3,6 = 482
Sign 때 계산한 j_2,6 = 696 , j_3,6 = 482

Verify 과정 j_2,7 = 633*a + 848 , j_3,7 = 494
Sign 때 계산한 j_2,7 = 633*a + 848 , j_3,7 = 494

Verify 과정 j_2,8 = 230*a + 618 , j_3,8 = 633*a + 848
Sign 때 계산한 j_2,8 = 230*a + 618 , j_3,8 = 633*a + 848

Verify 과정 j_2,9 = 633*a + 848 , j_3,9 = 494
Sign 때 계산한 j_2,9 = 633*a + 848 , j_3,9 = 494

Verify 과정 j_2,10 = 257 , j_3,10 = 232*a + 541
Sign 때 계산한 j_2,10 = 257 , j_3,10 = 232*a + 541

Verify 과정 j_2,11 = 348*a + 368 , j_3,11 = 803*a + 599
Sign 때 계산한 j_2,11 = 348*a + 368 , j_3,11 = 803*a + 599

Verify 과정 j_2,12 = 520*a + 114 , j_3,12 = 250*a + 693
Sign 때 계산한 j_2,12 = 520*a + 114 , j_3,12 = 250*a + 693

Verify 과정 j_2,13 = 281*a + 827 , j_3,13 = 451*a + 551
Sign 때 계산한 j_2,13 = 281*a + 827 , j_3,13 = 451*a + 551

Verify 과정 j_2,14 = 412*a + 139 , j_3,14 = 740*a + 293
Sign 때 계산한 j_2,14 = 412*a + 139 , j_3,14 = 740*a + 293

Verify 과정 j_2,15 = 348*a + 368 , j_3,15 = 803*a + 599
Sign 때 계산한 j_2,15 = 348*a + 368 , j_3,15 = 803*a + 599

Verify 과정 j_2,16 = 348*a + 368 , j_3,16 = 152*a + 605
Sign 때 계산한 j_2,16 = 348*a + 368 , j_3,16 = 152*a + 605

Verify 과정 j_2,17 = 348*a + 368 , j_3,17 = 803*a + 599
Sign 때 계산한 j_2,17 = 348*a + 368 , j_3,17 = 803*a + 599

Verify 과정 j_2,18 = 390*a + 617 , j_3,18 = 406*a + 197
Sign 때 계산한 j_2,18 = 390*a + 617 , j_3,18 = 406*a + 197

Verify 과정 j_2,19 = 343*a + 634 , j_3,19 = 406*a + 197

```
Sign 때 계산한 j_2,19 = 343*a + 634 , j_3,19 = 406*a + 197

Verify 과정 j_2,20 = 520*a + 114 , j_3,20 = 250*a + 693
Sign 때 계산한 j_2,20 = 520*a + 114 , j_3,20 = 250*a + 693

...

Verify 과정 j_2,109 = 343*a + 634 , j_3,109 = 406*a + 197
Sign 때 계산한 j_2,109 = 343*a + 634 , j_3,109 = 406*a + 197

Verify 과정 j_2,110 = 515*a + 716 , j_3,110 = 548*a + 32
Sign 때 계산한 j_2,110 = 515*a + 716 , j_3,110 = 548*a + 32

Verify 과정 j_2,111 = 451*a + 551 , j_3,111 = 371*a + 206
Sign 때 계산한 j_2,111 = 451*a + 551 , j_3,111 = 371*a + 206

Verify 과정 j_2,112 = 257 , j_3,112 = 232*a + 541
Sign 때 계산한 j_2,112 = 257 , j_3,112 = 232*a + 541

Verify 과정 j_2,113 = 633*a + 848 , j_3,113 = 494
Sign 때 계산한 j_2,113 = 633*a + 848 , j_3,113 = 494

Verify 과정 j_2,114 = 230*a + 618 , j_3,114 = 633*a + 848
Sign 때 계산한 j_2,114 = 230*a + 618 , j_3,114 = 633*a + 848

Verify 과정 j_2,115 = 419*a + 148 , j_3,115 = 509*a + 781
Sign 때 계산한 j_2,115 = 419*a + 148 , j_3,115 = 509*a + 781

Verify 과정 j_2,116 = 348*a + 368 , j_3,116 = 152*a + 605
Sign 때 계산한 j_2,116 = 348*a + 368 , j_3,116 = 152*a + 605

Verify 과정 j_2,117 = 451*a + 551 , j_3,117 = 590*a + 114
Sign 때 계산한 j_2,117 = 451*a + 551 , j_3,117 = 590*a + 114

Verify 과정 j_2,118 = 419*a + 148 , j_3,118 = 509*a + 781
Sign 때 계산한 j_2,118 = 419*a + 148 , j_3,118 = 509*a + 781

Verify 과정 j_2,119 = 390*a + 617 , j_3,119 = 527*a + 557
Sign 때 계산한 j_2,119 = 390*a + 617 , j_3,119 = 527*a + 557

Verify 과정 j_2,120 = 633*a + 848 , j_3,120 = 494
Sign 때 계산한 j_2,120 = 633*a + 848 , j_3,120 = 494

Verify 과정 j_2,121 = 473*a + 144 , j_3,121 = 657*a + 665
Sign 때 계산한 j_2,121 = 473*a + 144 , j_3,121 = 657*a + 665

Verify 과정 j_2,122 = 633*a + 848 , j_3,122 = 494
Sign 때 계산한 j_2,122 = 633*a + 848 , j_3,122 = 494

Verify 과정 j_2,123 = 348*a + 368 , j_3,123 = 803*a + 599
Sign 때 계산한 j_2,123 = 348*a + 368 , j_3,123 = 803*a + 599

Verify 과정 j_2,124 = 696 , j_3,124 = 853*a + 60
Sign 때 계산한 j_2,124 = 696 , j_3,124 = 853*a + 60

Verify 과정 j_2,125 = 412*a + 139 , j_3,125 = 740*a + 293
Sign 때 계산한 j_2,125 = 412*a + 139 , j_3,125 = 740*a + 293

Verify 과정 j_2,126 = 419*a + 148 , j_3,126 = 89
Sign 때 계산한 j_2,126 = 419*a + 148 , j_3,126 = 89

Verify 과정 j_2,127 = 419*a + 148 , j_3,127 = 509*a + 781
Sign 때 계산한 j_2,127 = 419*a + 148 , j_3,127 = 509*a + 781

Verify 과정 j_2,128 = 473*a + 144 , j_3,128 = 657*a + 665
Sign 때 계산한 j_2,128 = 473*a + 144 , j_3,128 = 657*a + 665

full_output.txt
```

j-invariant equalitiy check

```
print(J2 == J2_VERIFY)          ########  j_2,i : verifyier check
print(J3 == J3_VERIFY)          ########  j_3,i : verifyier check
```

```
True
True
```

Hash equality check

```
h == Hash(m + J2_VERIFY + J3_VERIFY)      ##### hash value equality check
```

```
True
```

< Attack >

```
print('z = {} \n, m = {} \n, h = {} \n, P1_tilda = {} \n, S2_tilda = {} \n, R2_tilda = {} \n, S2_tilda_prime = {} \n,
R2_tilda_prime = {} \n, f_iso = {} \n, f_inv = {} \n'.format( z,m , h , P1_tilda , S2_tilda , R2_tilda ,S2_tilda_prime ,
R2_tilda_prime , f_iso , f_inv ))  ### attack information
```

```
z = ['index', (515*a + 716, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (285*a+129)*x + (507*a+262) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(713*a+733)*x + (70*a+235) over Finite Field in a of size 863^2,
232*a + 541), 5, (473*a + 144, Isogeny of degree 16 from Elliptic
Curve defined by y^2 = x^3 + (156*a+400)*x + (395*a+233) over Finite
Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(566*a+536)*x + (566*a+723) over Finite Field in a of size 863^2,
657*a + 665), (451*a + 551, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (128*a+738)*x + (528*a+725) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(383*a+296)*x + (792*a+719) over Finite Field in a of size 863^2,
590*a + 114), (419*a + 148, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2,
89), 12, (633*a + 848, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2,
494), (230*a + 618, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (580*a+353)*x +
(76*a+790) over Finite Field in a of size 863^2, 633*a + 848), 25,
13, 0, 19, (281*a + 827, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (741*a+520)*x + (603*a+610) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(59*a+483)*x + (212*a+305) over Finite Field in a of size 863^2,
451*a + 551), 24, 27, 17, 27, (390*a + 617, Isogeny of degree 16
from Elliptic Curve defined by y^2 = x^3 + (707*a+556)*x +
(468*a+628) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (209*a+216)*x + (142*a+433) over Finite Field
in a of size 863^2, 406*a + 197), (343*a + 634, Isogeny of degree 16
from Elliptic Curve defined by y^2 = x^3 + (501*a+615)*x +
(587*a+427) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (551*a+484)*x + (778*a+382) over Finite Field
in a of size 863^2, 406*a + 197), 19, 7, 7, 3, (696, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + 242*x + 608
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (632*a+237)*x + (53*a+712) over Finite Field in a of
size 863^2, 482), 9, (281*a + 827, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (741*a+520)*x + (603*a+610)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (59*a+483)*x + (212*a+305) over Finite Field in a of
size 863^2, 451*a + 551), (473*a + 144, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + (156*a+400)*x + (395*a+233)
over Finite Field in a of size 863^2 to Elliptic Curve defined by
y^2 = x^3 + (566*a+536)*x + (566*a+723) over Finite Field in a of
size 863^2, 657*a + 665), 22, (473*a + 144, Isogeny of degree 16
from Elliptic Curve defined by y^2 = x^3 + (156*a+400)*x +
(468*a+630) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (456*a+133)*x + (29*a+65) over Finite Field
in a of size 863^2, 657*a + 665), (696, Isogeny of degree 16 from
Elliptic Curve defined by y^2 = x^3 + 242*x + 608 over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(632*a+237)*x + (53*a+712) over Finite Field in a of size 863^2,
482), (257, Isogeny of degree 16 from Elliptic Curve defined by y^2
= x^3 + (690*a+584)*x + (227*a+410) over Finite Field in a of size
863^2 to Elliptic Curve defined by y^2 = x^3 + (766*a+480)*x +
(453*a+761) over Finite Field in a of size 863^2, 232*a + 541),
(348*a + 368, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (768*a+443)*x +
(782*a+752) over Finite Field in a of size 863^2, 803*a + 599),
(348*a + 368, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (768*a+443)*x +
(782*a+752) over Finite Field in a of size 863^2, 803*a + 599),
(444*a + 567, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (389*a+152)*x + (383*a+717) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (336*a+306)*x +
(852*a+126) over Finite Field in a of size 863^2, 22), 8, 0, (390*a
+ 617, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3
+ (707*a+556)*x + (395*a+235) over Finite Field in a of size 863^2
to Elliptic Curve defined by y^2 = x^3 + (769*a+127)*x + (483*a+583)
over Finite Field in a of size 863^2, 527*a + 557), 16, 14, 12, 15,
8, (419*a + 148, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (474*a+541)*x + (383*a+626) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (11*a+341)*x +
(854*a+259) over Finite Field in a of size 863^2, 509*a + 781), 11,
(412*a + 139, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (735*a+3)*x + (528*a+473) over Finite Field in a of size
863^2 to Elliptic Curve defined by y^2 = x^3 + (846*a+213)*x +
```

(279*a+135) over Finite Field in a of size 863^2, 527*a + 557), 11, 25, 16, (241, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + 649*x + (594*a+566) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (474*a+642)*x + (89*a+114) over Finite Field in a of size 863^2, 803*a + 599), (419*a + 148, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2, 89), 17, 19, 11, (696, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + 242*x + 255 over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (710*a+204)*x + (814*a+648) over Finite Field in a of size 863^2, 853*a + 60), (582*a + 245, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (122*a+398)*x + (603*a+513) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (220*a+564)*x + (163*a+371) over Finite Field in a of size 863^2, 509*a + 781), (515*a + 716, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (285*a+129)*x + (507*a+262) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (713*a+733)*x + (70*a+235) over Finite Field in a of size 863^2, 232*a + 541), 4, 26, (241, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + 649*x + (594*a+566) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (474*a+642)*x + (89*a+114) over Finite Field in a of size 863^2, 803*a + 599), (390*a + 617, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (707*a+556)*x + (395*a+235) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (769*a+127)*x + (483*a+583) over Finite Field in a of size 863^2, 527*a + 557), 0, (451*a + 551, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (128*a+738)*x + (335*a+138) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (202*a+65)*x + (645*a+721) over Finite Field in a of size 863^2, 371*a + 206), 21, 19, 6, 2, 4, 15, 12, (419*a + 148, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2, 89), (348*a + 368, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (768*a+443)*x + (782*a+752) over Finite Field in a of size 863^2, 803*a + 599), (520*a + 114, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (362*a+253)*x + (587*a+712) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (42*a+735)*x + (103*a+540) over Finite Field in a of size 863^2, 250*a + 693), 15, (515*a + 716, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (285*a+129)*x + (356*a+601) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (686*a+292)*x + (679*a+591) over Finite Field in a of size 863^2, 548*a + 32), 18, (230*a + 618, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (580*a+353)*x + (76*a+790) over Finite Field in a of size 863^2, 633*a + 848), 3, 19, 15, (343*a + 634, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (501*a+615)*x + (587*a+427) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (551*a+484)*x + (778*a+382) over Finite Field in a of size 863^2, 406*a + 197), 23, 13, 13, (241, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + 649*x + (594*a+566) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (474*a+642)*x + (89*a+114) over Finite Field in a of size 863^2, 803*a + 599), (633*a + 848, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2, 494), (412*a + 139, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (735*a+3)*x + (335*a+390) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (467*a+299)*x + (409*a+790) over Finite Field in a of size 863^2, 740*a + 293), 4, 15, (473*a + 144, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (156*a+400)*x + (468*a+630) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (456*a+133)*x + (29*a+65) over Finite Field in a of size 863^2, 657*a + 665), 20, 3, 12, 13, 10, 19, 18, 10, (419*a + 148, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2, 89), (390*a + 617, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (707*a+556)*x + (468*a+628) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (209*a+216)*x + (142*a+433) over Finite Field in a of size 863^2, 406*a + 197), (419*a + 148, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (474*a+541)*x + (383*a+626) over Finite Field in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 + (11*a+341)*x + (854*a+259) over Finite Field in a of size 863^2, 509*a + 781), (343*a + 634, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 + (501*a+615)*x + (587*a+427) over Finite Field in a of size 863^2 to

```
Elliptic Curve defined by y^2 = x^3 + (551*a+484)*x + (778*a+382)
over Finite Field in a of size 863^2, 406*a + 197), 5, (473*a + 144,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(156*a+400)*x + (395*a+233) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (566*a+536)*x + (566*a+723)
over Finite Field in a of size 863^2, 657*a + 665), 11, 13, 13, 24,
(582*a + 245, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (122*a+398)*x + (603*a+513) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (220*a+564)*x +
(163*a+371) over Finite Field in a of size 863^2, 509*a + 781),
(343*a + 634, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (501*a+615)*x + (587*a+427) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (551*a+484)*x +
(778*a+382) over Finite Field in a of size 863^2, 406*a + 197), 14,
8, 13, (633*a + 848, Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2,
494), (230*a + 618, Isogeny of degree 16 from Elliptic Curve defined
by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (580*a+353)*x +
(76*a+790) over Finite Field in a of size 863^2, 633*a + 848), 3,
(348*a + 368, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (578*a+414)*x + (507*a+94) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (89*a+584)*x +
(75*a+76) over Finite Field in a of size 863^2, 152*a + 605), 18, 3,
(390*a + 617, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (707*a+556)*x + (395*a+235) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (769*a+127)*x +
(483*a+583) over Finite Field in a of size 863^2, 527*a + 557),
(633*a + 848, Isogeny of degree 16 from Elliptic Curve defined by
y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field in a of
size 863^2 to Elliptic Curve defined by y^2 = x^3 + (268*a+786)*x +
(563*a+138) over Finite Field in a of size 863^2, 494), (473*a +
144, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(156*a+400)*x + (468*a+630) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (456*a+133)*x + (29*a+65) over
Finite Field in a of size 863^2, 657*a + 665), 25, (348*a + 368,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(578*a+414)*x + (356*a+769) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (768*a+443)*x + (782*a+752)
over Finite Field in a of size 863^2, 803*a + 599), 11, (412*a +
139, Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(735*a+3)*x + (335*a+390) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (467*a+299)*x + (409*a+790)
over Finite Field in a of size 863^2, 740*a + 293), (419*a + 148,
Isogeny of degree 16 from Elliptic Curve defined by y^2 = x^3 +
(474*a+541)*x + (480*a+237) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (723*a+588)*x + (454*a+255)
over Finite Field in a of size 863^2, 89), (419*a + 148, Isogeny of
degree 16 from Elliptic Curve defined by y^2 = x^3 + (474*a+541)*x +
(383*a+626) over Finite Field in a of size 863^2 to Elliptic Curve
defined by y^2 = x^3 + (11*a+341)*x + (854*a+259) over Finite Field
in a of size 863^2, 509*a + 781), 6]
, m = isogeny
, h =
10111011000010000110000101101111110010000010100011000111001101000000₩
01110101000100011100100000000111101000011000110100111010110
, P1_tilda = (256*a + 404 : 23*a + 425 : 1)
, S2_tilda = (603*a + 31 : 164*a + 224 : 1)
, R2_tilda = (636*a + 736 : 825*a + 34 : 1)
, S2_tilda_prime = (830*a + 379 : 680*a + 602 : 1)
, R2_tilda_prime = (213*a + 705 : 795*a + 677 : 1)
, f_iso = <function f_iso at 0x7f274e4218c0>
, f_inv = <function f_inv at 0x7f274e421a28>
```

```
R2_tilda in E0_prime
```

```
True
```

```
j2_attack = ['index']      ####### j'_2,i = j2_attack[i]
j3_attack = ['index']      ####### j'_3,i = j3_attack[i]
attack_isogeny2 =  ['index']
attack_isogeny3 =  ['index']


for i in range(1,t+1):

    if h[i-1] == '0' :                                                                                  ###### b_i =
0  i.e, z_i = α_i Case


        attack_isogeny2.append(EllipticCurveIsogeny(E0_prime, R2_tilda + z[i]*S2_tilda))
        j2_attack.append(EllipticCurveIsogeny(E0_prime, R2_tilda + z[i]*S2_tilda).codomain().j_invariant())          ######
domain E0' , kernel R2 + [z_i]S2 -->isogeny -->j'_2,i

        attack_isogeny3.append(EllipticCurveIsogeny(E1_prime, R2_tilda_prime + z[i]*S2_tilda_prime))
```

```
        j3_attack.append(EllipticCurveIsogeny(E1_prime, R2_tilda_prime + z[i]*S2_tilda_prime).codomain().j_invariant())
###### domain E1' , kernel R'2 + [z_i]S'2 --> isogeny --> j_3,i


    else:

                                                                                                                    ###### b_i = 1
i.e, z_i = j_2,i  Case

        attack_isogeny2.append("none")
        j2_attack.append(z[i][0])                                                                                     ###### j_2,i
= z_i

        attack_isogeny3.append(EllipticCurveIsogeny(E2[i] , psi[i](f_inv(P1_tilda))))
        j3_attack.append(EllipticCurveIsogeny(E2[i] , psi[i](f_inv(P1_tilda))).codomain().j_invariant())      ###### domain
E_2,i , kernel Ψ_i(f(P_tilda)) --> isogeny --> j_3,i


J2_ATTACK = ''                  ########## J2_ATTACK = j_2,i_attack all sequences
J3_ATTACK = ''                  ########## J3_ATTACK = j_3,i_attack all sequences

for j2_att in j2_attack[1:]:
    J2_ATTACK += str(j2_att)
for j3_att in j3_attack[1:]:
    J3_ATTACK += str(j3_att)
```

For attack, isogeny

```
for i in range(1,t+1):
    print("j_2,{} 계산 때 쓰인 isogeny  = {}".format(i,attack_isogeny2[i]))
    print("j_3,{} 계산 때 쓰인 isogeny  = {}₩n".format(i,attack_isogeny3[i]))
```

```
WARNING: Output truncated!
full output.txt


j_2,1 계산 때 쓰인 isogeny  = none
j_3,1 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (285*a+129)*x + (507*a+262) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(713*a+733)*x + (70*a+235) over Finite Field in a of size 863^2

j_2,2 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (312*a+800)*x + (200*a+402)
over Finite Field in a of size 863^2
j_3,2 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(505*a+399)*x + (802*a+637) over Finite Field in a of size 863^2

j_2,3 계산 때 쓰인 isogeny  = none
j_3,3 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (156*a+400)*x + (395*a+233) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(566*a+536)*x + (566*a+723) over Finite Field in a of size 863^2

j_2,4 계산 때 쓰인 isogeny  = none
j_3,4 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (128*a+738)*x + (528*a+725) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(383*a+296)*x + (792*a+719) over Finite Field in a of size 863^2

j_2,5 계산 때 쓰인 isogeny  = none
j_3,5 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2

j_2,6 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + 484*x + 577 over Finite Field
in a of size 863^2
j_3,6 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(170*a+711)*x + (692*a+764) over Finite Field in a of size 863^2

j_2,7 계산 때 쓰인 isogeny  = none
j_3,7 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2
```

```
j_2,8 계산 때 쓰인 isogeny  = none
j_3,8 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(580*a+353)*x + (76*a+790) over Finite Field in a of size 863^2

j_2,9 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (83*a+519)*x + (23*a+692) over
Finite Field in a of size 863^2
j_3,9 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(804*a+632)*x + (512*a+662) over Finite Field in a of size 863^2

j_2,10 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (517*a+305)*x + (38*a+426)
over Finite Field in a of size 863^2
j_3,10 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(572*a+577)*x + (297*a+36) over Finite Field in a of size 863^2

j_2,11 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (293*a+828)*x + (71*a+277)
over Finite Field in a of size 863^2
j_3,11 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(578*a+466)*x + (587*a+293) over Finite Field in a of size 863^2

j_2,12 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (724*a+506)*x + (391*a+142)
over Finite Field in a of size 863^2
j_3,12 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(126*a+479)*x + (319*a+114) over Finite Field in a of size 863^2

j_2,13 계산 때 쓰인 isogeny  = none
j_3,13 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (741*a+520)*x + (603*a+610) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(59*a+483)*x + (212*a+305) over Finite Field in a of size 863^2

j_2,14 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (607*a+6)*x + (748*a+742) over
Finite Field in a of size 863^2
j_3,14 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(538*a+34)*x + (211*a+838) over Finite Field in a of size 863^2

j_2,15 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (293*a+828)*x + (71*a+277)
over Finite Field in a of size 863^2
j_3,15 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(578*a+466)*x + (587*a+293) over Finite Field in a of size 863^2

j_2,16 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (293*a+828)*x + (792*a+586)
over Finite Field in a of size 863^2
j_3,16 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(267*a+26)*x + (735*a+227) over Finite Field in a of size 863^2

j_2,17 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (293*a+828)*x + (71*a+277)
over Finite Field in a of size 863^2
j_3,17 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(578*a+466)*x + (587*a+293) over Finite Field in a of size 863^2

j_2,18 계산 때 쓰인 isogeny  = none
j_3,18 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
```

```
defined by y^2 = x^3 + (707*a+556)*x + (468*a+628) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(209*a+216)*x + (142*a+433) over Finite Field in a of size 863^2

j_2,19 계산 때 쓰인 isogeny  = none
j_3,19 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (501*a+615)*x + (587*a+427) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(551*a+484)*x + (778*a+382) over Finite Field in a of size 863^2

j_2,20 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (724*a+506)*x + (391*a+142)
over Finite Field in a of size 863^2
j_3,20 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(126*a+479)*x + (319*a+114) over Finite Field in a of size 863^2

...

j_2,109 계산 때 쓰인 isogeny  = none
j_3,109 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (501*a+615)*x + (587*a+427) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(551*a+484)*x + (778*a+382) over Finite Field in a of size 863^2

j_2,110 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (570*a+258)*x + (71*a+515)
over Finite Field in a of size 863^2
j_3,110 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(332*a+13)*x + (268*a+96) over Finite Field in a of size 863^2

j_2,111 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (256*a+613)*x + (748*a+236)
over Finite Field in a of size 863^2
j_3,111 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(606*a+195)*x + (280*a+507) over Finite Field in a of size 863^2

j_2,112 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (517*a+305)*x + (38*a+426)
over Finite Field in a of size 863^2
j_3,112 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(572*a+577)*x + (297*a+36) over Finite Field in a of size 863^2

j_2,113 계산 때 쓰인 isogeny  = none
j_3,113 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2

j_2,114 계산 때 쓰인 isogeny  = none
j_3,114 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (390*a+301)*x + (796*a+657) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(580*a+353)*x + (76*a+790) over Finite Field in a of size 863^2

j_2,115 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (85*a+219)*x + (680*a+120)
over Finite Field in a of size 863^2
j_3,115 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(33*a+160)*x + (257*a+467) over Finite Field in a of size 863^2

j_2,116 계산 때 쓰인 isogeny  = none
j_3,116 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (578*a+414)*x + (507*a+94) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(89*a+584)*x + (75*a+76) over Finite Field in a of size 863^2

j_2,117 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (256*a+613)*x + (115*a+627)
over Finite Field in a of size 863^2
j_3,117 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
```

```
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(286*a+25)*x + (685*a+660) over Finite Field in a of size 863^2

j_2,118 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (85*a+219)*x + (680*a+120)
over Finite Field in a of size 863^2
j_3,118 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(33*a+160)*x + (257*a+467) over Finite Field in a of size 863^2

j_2,119 계산 때 쓰인 isogeny  = none
j_3,119 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (707*a+556)*x + (395*a+235) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(769*a+127)*x + (483*a+583) over Finite Field in a of size 863^2

j_2,120 계산 때 쓰인 isogeny  = none
j_3,120 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (473*a+691)*x + (796*a+273) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(268*a+786)*x + (563*a+138) over Finite Field in a of size 863^2

j_2,121 계산 때 쓰인 isogeny  = none
j_3,121 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (156*a+400)*x + (468*a+630) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(456*a+133)*x + (29*a+65) over Finite Field in a of size 863^2

j_2,122 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (83*a+519)*x + (23*a+692) over
Finite Field in a of size 863^2
j_3,122 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(804*a+632)*x + (512*a+662) over Finite Field in a of size 863^2

j_2,123 계산 때 쓰인 isogeny  = none
j_3,123 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (578*a+414)*x + (356*a+769) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(768*a+443)*x + (782*a+752) over Finite Field in a of size 863^2

j_2,124 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + 484*x + 286 over Finite Field
in a of size 863^2
j_3,124 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(404*a+612)*x + (728*a+482) over Finite Field in a of size 863^2

j_2,125 계산 때 쓰인 isogeny  = none
j_3,125 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (735*a+3)*x + (335*a+390) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(467*a+299)*x + (409*a+790) over Finite Field in a of size 863^2

j_2,126 계산 때 쓰인 isogeny  = none
j_3,126 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (480*a+237) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(723*a+588)*x + (454*a+255) over Finite Field in a of size 863^2

j_2,127 계산 때 쓰인 isogeny  = none
j_3,127 계산 때 쓰인 isogeny  = Isogeny of degree 16 from Elliptic Curve
defined by y^2 = x^3 + (474*a+541)*x + (383*a+626) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(11*a+341)*x + (854*a+259) over Finite Field in a of size 863^2

j_2,128 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + 2*x over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (312*a+800)*x + (663*a+461)
over Finite Field in a of size 863^2
j_3,128 계산 때 쓰인 isogeny  = Isogeny of degree 27 from Elliptic Curve
defined by y^2 = x^3 + (465*a+542)*x + (349*a+291) over Finite Field
in a of size 863^2 to Elliptic Curve defined by y^2 = x^3 +
(835*a+745)*x + (714*a+354) over Finite Field in a of size 863^2

full_output.txt
```

Get isogeny (ex : j_2,5 , j_3,5 : isogeny)

```
attack_isogeny2[5] ; attack_isogeny3[6]
```

```
'none'
Isogeny of degree 27 from Elliptic Curve defined by y^2 = x^3 +
(465*a+542)*x + (349*a+291) over Finite Field in a of size 863^2 to
Elliptic Curve defined by y^2 = x^3 + (170*a+711)*x + (692*a+764)
over Finite Field in a of size 863^2
```

```
for i in range(1,t+1):
    print("Attack 과정 때 계산한 j_2,{} = {} , j_3,{} = {} WnSign 때 계산한 j_2,{} = {} , j_3,{} =
{}₩n".format(i,j2_attack[i],i,j3_attack[i],i,j2[i],i,j3[i]))
```

```
WARNING: Output truncated!
full_output.txt
```

```
Attack 과정 때 계산한 j_2,1 = 515*a + 716 , j_3,1 = 232*a + 541
Sign 때 계산한 j_2,1 = 515*a + 716 , j_3,1 = 232*a + 541

Attack 과정 때 계산한 j_2,2 = 473*a + 144 , j_3,2 = 657*a + 665
Sign 때 계산한 j_2,2 = 473*a + 144 , j_3,2 = 657*a + 665

Attack 과정 때 계산한 j_2,3 = 473*a + 144 , j_3,3 = 657*a + 665
Sign 때 계산한 j_2,3 = 473*a + 144 , j_3,3 = 657*a + 665

Attack 과정 때 계산한 j_2,4 = 451*a + 551 , j_3,4 = 590*a + 114
Sign 때 계산한 j_2,4 = 451*a + 551 , j_3,4 = 590*a + 114

Attack 과정 때 계산한 j_2,5 = 419*a + 148 , j_3,5 = 89
Sign 때 계산한 j_2,5 = 419*a + 148 , j_3,5 = 89

Attack 과정 때 계산한 j_2,6 = 696 , j_3,6 = 482
Sign 때 계산한 j_2,6 = 696 , j_3,6 = 482

Attack 과정 때 계산한 j_2,7 = 633*a + 848 , j_3,7 = 494
Sign 때 계산한 j_2,7 = 633*a + 848 , j_3,7 = 494

Attack 과정 때 계산한 j_2,8 = 230*a + 618 , j_3,8 = 633*a + 848
Sign 때 계산한 j_2,8 = 230*a + 618 , j_3,8 = 633*a + 848

Attack 과정 때 계산한 j_2,9 = 633*a + 848 , j_3,9 = 494
Sign 때 계산한 j_2,9 = 633*a + 848 , j_3,9 = 494

Attack 과정 때 계산한 j_2,10 = 257 , j_3,10 = 232*a + 541
Sign 때 계산한 j_2,10 = 257 , j_3,10 = 232*a + 541

Attack 과정 때 계산한 j_2,11 = 348*a + 368 , j_3,11 = 803*a + 599
Sign 때 계산한 j_2,11 = 348*a + 368 , j_3,11 = 803*a + 599

Attack 과정 때 계산한 j_2,12 = 520*a + 114 , j_3,12 = 250*a + 693
Sign 때 계산한 j_2,12 = 520*a + 114 , j_3,12 = 250*a + 693

Attack 과정 때 계산한 j_2,13 = 281*a + 827 , j_3,13 = 451*a + 551
Sign 때 계산한 j_2,13 = 281*a + 827 , j_3,13 = 451*a + 551

Attack 과정 때 계산한 j_2,14 = 412*a + 139 , j_3,14 = 740*a + 293
Sign 때 계산한 j_2,14 = 412*a + 139 , j_3,14 = 740*a + 293

Attack 과정 때 계산한 j_2,15 = 348*a + 368 , j_3,15 = 803*a + 599
Sign 때 계산한 j_2,15 = 348*a + 368 , j_3,15 = 803*a + 599

Attack 과정 때 계산한 j_2,16 = 348*a + 368 , j_3,16 = 152*a + 605
Sign 때 계산한 j_2,16 = 348*a + 368 , j_3,16 = 152*a + 605

Attack 과정 때 계산한 j_2,17 = 348*a + 368 , j_3,17 = 803*a + 599
Sign 때 계산한 j_2,17 = 348*a + 368 , j_3,17 = 803*a + 599

Attack 과정 때 계산한 j_2,18 = 390*a + 617 , j_3,18 = 406*a + 197
Sign 때 계산한 j_2,18 = 390*a + 617 , j_3,18 = 406*a + 197

Attack 과정 때 계산한 j_2,19 = 343*a + 634 , j_3,19 = 406*a + 197
Sign 때 계산한 j_2,19 = 343*a + 634 , j_3,19 = 406*a + 197

Attack 과정 때 계산한 j_2,20 = 520*a + 114 , j_3,20 = 250*a + 693
Sign 때 계산한 j_2,20 = 520*a + 114 , j_3,20 = 250*a + 693

...

Attack 과정 때 계산한 j_2,109 = 343*a + 634 , j_3,109 = 406*a + 197
Sign 때 계산한 j_2,109 = 343*a + 634 , j_3,109 = 406*a + 197

Attack 과정 때 계산한 j_2,110 = 515*a + 716 , j_3,110 = 548*a + 32
Sign 때 계산한 j_2,110 = 515*a + 716 , j_3,110 = 548*a + 32
```

```
Attack 과정 때 계산한 j_2,111 = 451*a + 551 , j_3,111 = 371*a + 206
Sign 때 계산한 j_2,111 = 451*a + 551 , j_3,111 = 371*a + 206

Attack 과정 때 계산한 j_2,112 = 257 , j_3,112 = 232*a + 541
Sign 때 계산한 j_2,112 = 257 , j_3,112 = 232*a + 541

Attack 과정 때 계산한 j_2,113 = 633*a + 848 , j_3,113 = 494
Sign 때 계산한 j_2,113 = 633*a + 848 , j_3,113 = 494

Attack 과정 때 계산한 j_2,114 = 230*a + 618 , j_3,114 = 633*a + 848
Sign 때 계산한 j_2,114 = 230*a + 618 , j_3,114 = 633*a + 848

Attack 과정 때 계산한 j_2,115 = 419*a + 148 , j_3,115 = 509*a + 781
Sign 때 계산한 j_2,115 = 419*a + 148 , j_3,115 = 509*a + 781

Attack 과정 때 계산한 j_2,116 = 348*a + 368 , j_3,116 = 152*a + 605
Sign 때 계산한 j_2,116 = 348*a + 368 , j_3,116 = 152*a + 605

Attack 과정 때 계산한 j_2,117 = 451*a + 551 , j_3,117 = 590*a + 114
Sign 때 계산한 j_2,117 = 451*a + 551 , j_3,117 = 590*a + 114

Attack 과정 때 계산한 j_2,118 = 419*a + 148 , j_3,118 = 509*a + 781
Sign 때 계산한 j_2,118 = 419*a + 148 , j_3,118 = 509*a + 781

Attack 과정 때 계산한 j_2,119 = 390*a + 617 , j_3,119 = 527*a + 557
Sign 때 계산한 j_2,119 = 390*a + 617 , j_3,119 = 527*a + 557

Attack 과정 때 계산한 j_2,120 = 633*a + 848 , j_3,120 = 494
Sign 때 계산한 j_2,120 = 633*a + 848 , j_3,120 = 494

Attack 과정 때 계산한 j_2,121 = 473*a + 144 , j_3,121 = 657*a + 665
Sign 때 계산한 j_2,121 = 473*a + 144 , j_3,121 = 657*a + 665

Attack 과정 때 계산한 j_2,122 = 633*a + 848 , j_3,122 = 494
Sign 때 계산한 j_2,122 = 633*a + 848 , j_3,122 = 494

Attack 과정 때 계산한 j_2,123 = 348*a + 368 , j_3,123 = 803*a + 599
Sign 때 계산한 j_2,123 = 348*a + 368 , j_3,123 = 803*a + 599

Attack 과정 때 계산한 j_2,124 = 696 , j_3,124 = 853*a + 60
Sign 때 계산한 j_2,124 = 696 , j_3,124 = 853*a + 60

Attack 과정 때 계산한 j_2,125 = 412*a + 139 , j_3,125 = 740*a + 293
Sign 때 계산한 j_2,125 = 412*a + 139 , j_3,125 = 740*a + 293

Attack 과정 때 계산한 j_2,126 = 419*a + 148 , j_3,126 = 89
Sign 때 계산한 j_2,126 = 419*a + 148 , j_3,126 = 89

Attack 과정 때 계산한 j_2,127 = 419*a + 148 , j_3,127 = 509*a + 781
Sign 때 계산한 j_2,127 = 419*a + 148 , j_3,127 = 509*a + 781

Attack 과정 때 계산한 j_2,128 = 473*a + 144 , j_3,128 = 657*a + 665
Sign 때 계산한 j_2,128 = 473*a + 144 , j_3,128 = 657*a + 665

full_output.txt
```

j-invariant equality check

```
print(J2 == J2_ATTACK)          ########  j_2,i_ATTACK  =  j_2,i
print(J3 == J3_ATTACK)          ########  j_3,i_ATTACK =  j_3,i
```

```
True
True
```

Hash -->attack success check

```
h == Hash(m + J2_ATTACK + J3_ATTACK)      ##### hash value equality check
```

```
True
```