

# Week\_4 做题记录

- **Crypto**
  - ECC

# ECC

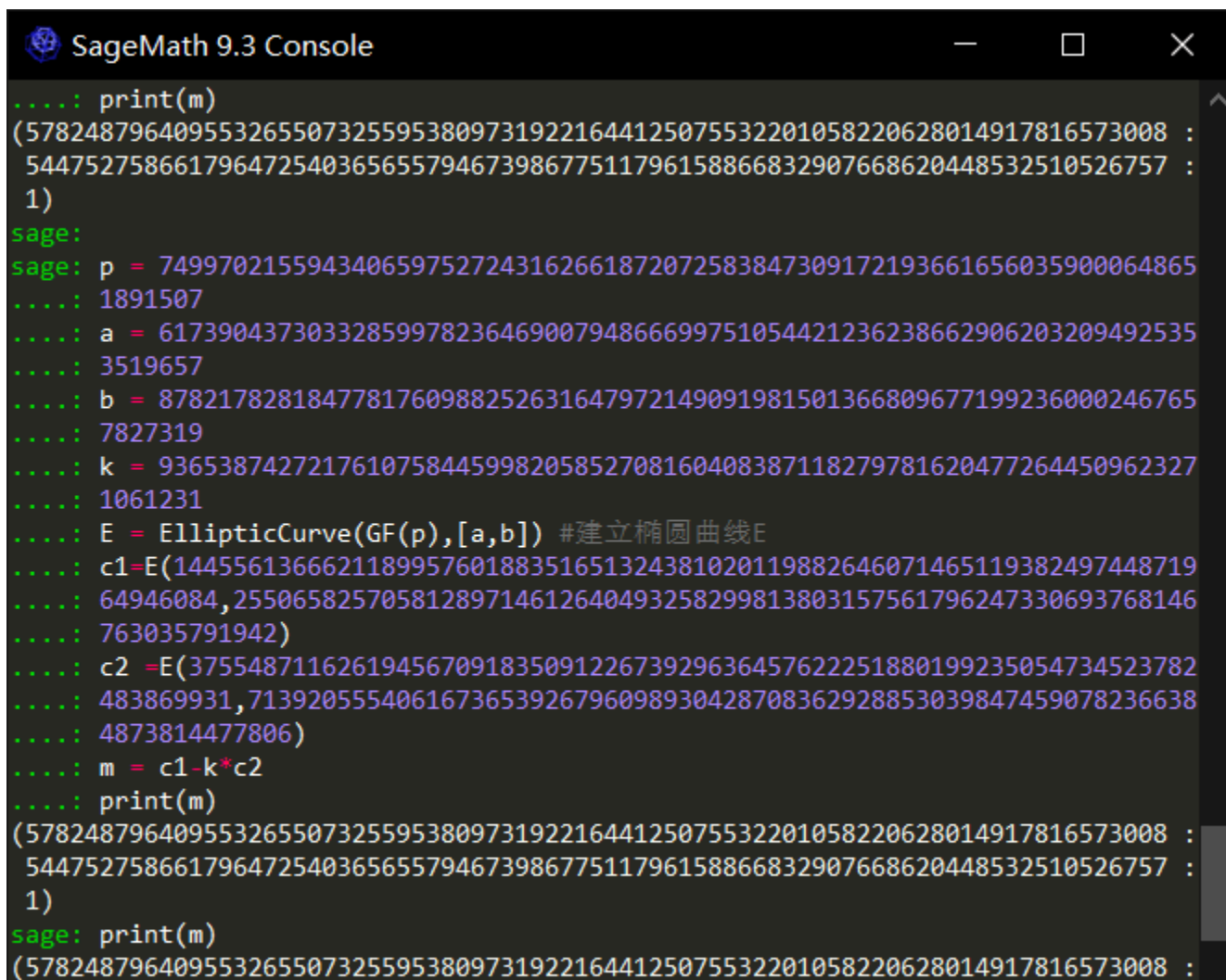
## • 思路

从题目得知ECC椭圆曲线加密，具体材料参考[ECC椭圆曲线加密算法—加解密（SageMath实现）](#)

## • 代码

```
p = 74997021559434065975272431626618720725838473091721936616560359000648651891507
a = 61739043730332859978236469007948666997510544212362386629062032094925353519657
b = 87821782818477817609882526316479721490919815013668096771992360002467657827319
k = 93653874272176107584459982058527081604083871182797816204772644509623271061231
E = EllipticCurve(GF(p),[a,b]) #建立椭圆曲线E
c1=E(14455613666211899576018835165132438102011988264607146511938249744871964946084,25506582570581289714612640493
c2 =E(37554871162619456709183509122673929636457622251880199235054734523782483869931,7139205554061673653926796098
m = c1-k*c2
print(m)
```

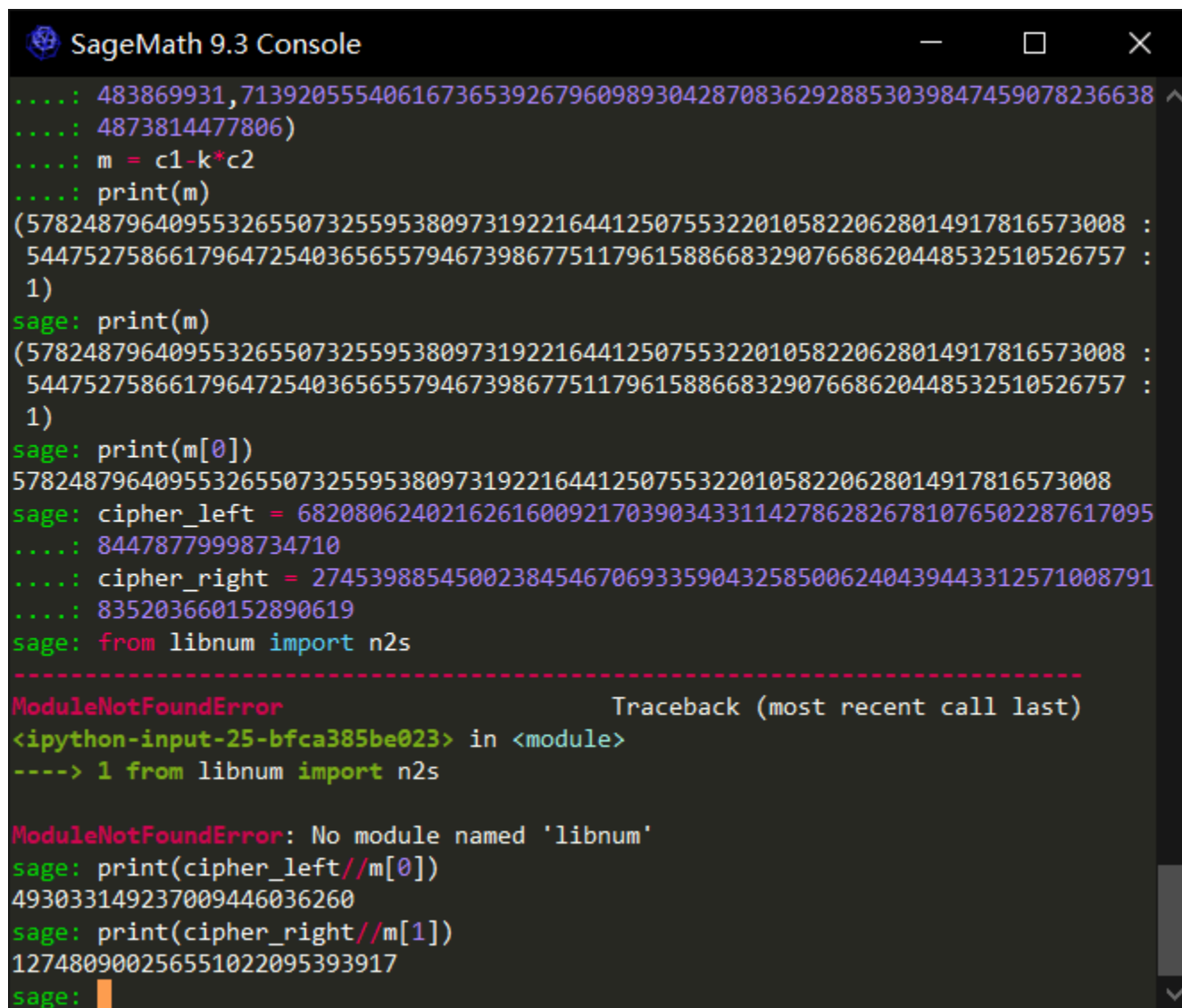
sagemath解出来得到m0, m1



```
SageMath 9.3 Console
.....: print(m)
(57824879640955326550732559538097319221644125075532201058220628014917816573008 :
54475275866179647254036565579467398677511796158866832907668620448532510526757 :
1)
sage:
sage: p = 7499702155943406597527243162661872072583847309172193661656035900064865
.....: 1891507
.....: a = 6173904373033285997823646900794866699751054421236238662906203209492535
.....: 3519657
.....: b = 8782178281847781760988252631647972149091981501366809677199236000246765
.....: 7827319
.....: k = 9365387427217610758445998205852708160408387118279781620477264450962327
.....: 1061231
.....: E = EllipticCurve(GF(p),[a,b]) #建立椭圆曲线E
.....: c1=E(144556136662118995760188351651324381020119882646071465119382497448719
.....: 64946084,25506582570581289714612640493258299813803157561796247330693768146
.....: 763035791942)
.....: c2 =E(37554871162619456709183509122673929636457622251880199235054734523782
.....: 483869931,7139205554061673653926796098930428708362928853039847459078236638
.....: 4873814477806)
.....: m = c1-k*c2
.....: print(m)
(57824879640955326550732559538097319221644125075532201058220628014917816573008 :
54475275866179647254036565579467398677511796158866832907668620448532510526757 :
1)
sage: print(m)
(57824879640955326550732559538097319221644125075532201058220628014917816573008 :
```

```
54475275866179647254036565579467398677511796158866832907668620448532510526757 :
1)
```

一开始我使用的python对密文进行除来转化发现没法转，后来了解到sagemath里的除法是带有模运算的（ $\text{left} = f * m[0] \% p$ ）用sagemath来除就没事了



```
SageMath 9.3 Console
.....: 483869931,7139205554061673653926796098930428708362928853039847459078236638
.....: 4873814477806)
.....: m = c1-k*c2
.....: print(m)
(57824879640955326550732559538097319221644125075532201058220628014917816573008 :
54475275866179647254036565579467398677511796158866832907668620448532510526757 :
1)
sage: print(m)
(57824879640955326550732559538097319221644125075532201058220628014917816573008 :
54475275866179647254036565579467398677511796158866832907668620448532510526757 :
1)
sage: print(m[0])
57824879640955326550732559538097319221644125075532201058220628014917816573008
sage: cipher_left = 682080624021626160092170390343311427862826781076502287617095
.....: 84478779998734710
.....: cipher_right = 27453988545002384546706933590432585006240439443312571008791
.....: 835203660152890619
sage: from libnum import n2s
-----
ModuleNotFoundError                                Traceback (most recent call last)
<ipython-input-25-bfca385be023> in <module>
----> 1 from libnum import n2s

ModuleNotFoundError: No module named 'libnum'
sage: print(cipher_left//m[0])
493033149237009446036260
sage: print(cipher_right//m[1])
127480900256551022095393917
sage: 
```

```
print(n2s(493033149237009446036260))
print(n2s(127480900256551022095393917))
```

```
# flag='hgame{Ecc$is!s0@HaRd}'
```