看雪2020CTF 守株待兔

原创

大帅锅1 于 2020-05-29 16:52:34 发布 169 收藏
分类专栏： CTF

本文链接：https://blog.csdn.net/qq_34905587/article/details/106428728

1. 子群的阶就是子群中的元素个数，等价于 $nP = 0$，其n是正整数，且n是其中最小的1个，这个n就是子群的阶。
2. 根据拉格朗日定理，子群P的阶，是父群阶的一个因子，比如一个椭圆曲线有N个元素，它的一个子群有n个元素，n能整除N

根据这句话，可以求分解曲线阶的最小公倍数即为整个曲线的阶

```
#n=379752279369436739228088727554456278545655366381 99 * 400946909509208810306837352927614683892148997240 61

#curve 1
M = 400946909509208810306837352927614683892148997240 61
A = 0
B = 0x68ef17c5878742e629b88277f8b712506f899964098f94bc39b54e21a5493d961c69171ee03dc2df71L % M
P = (0x4B58435446323032302E7265616479752E43617463682E5261626269743A757365726E616D65 % M, 0x2177C13E81BEACB0
F = GF(M)
E = EllipticCurve(F,[A,B])
print ('ECC1:',E)
P = E.point(P)
ord1=E.order()
print ('ord1:',factor(ord1))

#curve 2
M = 379752279369436739228088727554456278545655366381 99
A = 0
B = 0x68ef17c5878742e629b88277f8b712506f899964098f94bc39b54e21a5493d961c69171ee03dc2df71L %M
P = (0x4B58435446323032302E7265616479752E43617463682E5261626269743A757365726E616D65 % M, 0x2177C13E81BEACB0
F = GF(M)
E = EllipticCurve(F,[A,B])
print ('ECC2:',E)
P = E.point(P)
#Q = E.point(Q)
print ('ord2:',E.order())
P=E.point(P)
ord2=E.order()
order=lcm(ord1,ord2)

#curve
M = 379752279369436739228088727554456278545655366381 99 * 400946909509208810306837352927614683892148997240 61
A = 0
B = 0x68ef17c5878742e629b88277f8b712506f899964098f94bc39b54e21a5493d961c69171ee03dc2df71L
P = (0x4B58435446323032302E7265616479752E43617463682E5261626269743A757365726E616D65, 0x2177C13E81BEACB06B6D

F = Zmod(M)
E = EllipticCurve(F,[A,B])
P=E.point(P)

print ('ECC2:',E)
print ('ord2:',order)
print('P:',P)
print('P:',(order+1)*P)

Base=inverse_mod(257,order)*P
print('Base:',Base)
#after calc base
print("verifying P:",Base*257)
x,y,z=str(Base).replace('(','').replace(')','').split(' : ')
x=int(x)
y=int(y)

print("flag{username-"+hex(x)[2:-1].upper()+'-'+hex(y)[2:-1].upper()+'}')
#flag{username-27D9A3DACA0B408853CBB1D79393864648F4DEA917066285C182C8B717A6822D9B67A541F173F75DB88-12C1975E
```