2021虎符ctf crypto 密码学WP

原创

置顶 ljahum 于 2021-04-07 12:56:43 发布 593 收藏

分类专栏： ctf 文章标签： 线性代数 几何学 python

本文链接：https://blog.csdn.net/a_touhouer/article/details/115482994

ctf 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

看懂曲线变化的原理就比较简单了

基本上算学妹做出来的，tql

link wiki

这里整理一个通解公式来把玩

```
# sage
n = 6
a = (4*n ^ 2+12*n-3)
b = 32*(n+3)
ee = EllipticCurve([0, a, 0, b, 0])
# y2=x3+109x2+224x


def orig(P, N):
    x = P[0]
    y = P[1]
    a = (8*(N+3)-x+y)/(2*(N+3)*(4-x))
    b = (8*(N+3)-x-y)/(2*(N+3)*(4-x))
    c = (-4*(N+3)-(N+2)*x)/((N+3)*(4-x))
    da = denominator(a)
    db = denominator(b)
    dc = denominator(c)
    l = lcm(da, lcm(db, dc))
    return [a*l, b*l, c*l]


g = ee.gens()
# print(g)
# [(-200 : 680 : 1)]
P = ee(-200, 680)
# P = ee(g)
# print(P)
for i in range(1,100):
    x,y,z = orig(i*P, n)
    if(x>0 and y>0 and z>0):
        print(f'x={x}\ny={y}\nz={z}\n')
        print((x/(y+z))+(z/(x+y))+(y/(x+z)))
        print(f'i = {i}')
        break
```