Fintech HW3

R11922196 林佑鑫

Q1:

(10338857399563508035974916425421659830878883530402360147780309523428649499368 3,

787349480920740724105556683778235783031297677369394103695842975796530058616 45)

```
F = FiniteField(0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F)
C = EllipticCurve([F(0), F(7)])
G = C.lift_x(0x79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798)
N = FiniteField(C.order())
d = 2196

print(4*G)
```

```
(10338857399563508035974916425421659830878883530402360147780309523428649499368 3 : 787349480920740724105556683778235783031297677369394103695842975796530058616 45 : 1)
```

Q2:

(21505829891763648114329055987619236494102133314575206970830385799158076338148,

177883805585535741898877445056070477242430973427664252339276990875988710915 45)

```
F = FiniteField(0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F)
C = EllipticCurve([F(0), F(7)])
G = C.lift_x(0x79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798)
N = FiniteField(C.order())
d = 2196

print(5*G)
```

```
(21505829891763648114329055987619236494102133314575206970830385799158076338148 : 177883805585535741898877445056070477242430973427664252339276990875988710915 45 : 1)
```

Q3:

(7338292215331370827335348891068137621101936635261179149511083770133973870233 1,

112326790001062152217762067843865999180996379321494205852276961943359818100985)

```
F = FiniteField(0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F)
C = EllipticCurve([F(0), F(7)])
G = C.lift_x(0x79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798)
N = FiniteField(C.order())
d = 2196

print(d*G)
```

```
(7338292215331370827335348891068137621101936635261179149511083770133973870233 1 : 112326790001062152217762067843865999180996379321494205852276961943359818100985 : 1)
```

Q4:

d = 2196, binary(d) = 100010010100

Doubles: 11, Additions: 3

Q5:

Doubles: 11, Additions: 3

Binary format 1 的數量較少，用反元素來運算並沒有比較快

Q6, Q7:

k = 109740109892235532878306356133800093045252333191458370520279557037312996874868

d = 2196

r = 70000326365577208095100227701225545430768716907230157761227603089793312808504

s = 71612401756312716822803358871590990690042855586470157310817110099955546623103

verify: True

```
F = FiniteField(0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F)
C = EllipticCurve([F(0), F(7)])
G = C.lift_x(0x79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798)
N = FiniteField(C.order())
n = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141
d = 2196
Q = d*G

def sign(z):
    r = 0
    s = 0
    while s == 0:
        k = 1
        while r == 0:
            k = N.random_element()
            (x1, y1) = (int(k)*G).xy()
            r = x1
        s = k^(-1)*(z+N(r)*d)
    print(f'random k: {k}')
    return r, s

def verify(z, r, s):
    w = N(s) ^ (-1)
    u1 = int(z * w); u2 = int(N(r) * w)
    (x1, y1) = (u1*G + u2*Q).xy()
    return r == x1

e = 0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
z = 0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

r, s = sign(z)
print(f'r: {r}\ns: {s}')
print(verify(z, r, s))
```

```
random k: 109740109892235532878306356133800093045252333191458370520279557037312996874868
r: 70000326365577208095100227701225545430768716907230157761227603089793312808504
s: 71612401756312716822803358871590990690042855586470157310817110099955546623103
True
```

Q8:

p(1) = 10, p(2) = 20, p(3) = 2196

f(x) = 10 * (x^2 - 5*x + 6) * 5004 + 20 * (x^2 – 4*x + 3) * 10006 + 2196 * (x^2 – 3*x + 2) * 3336

= 7576016 * x^2 – 23028248 * x + 15552312