ECC 3rd homework

김동휘, 박태원, 송유석

Finite Field

- **목표 : FiniteField 클래스를 구현**
  - 클래스 생성시 입력값은 power, poly
  - GF(2^{power})의 Finite Field 생성만 고려하며, poly는 십진법으로 주어짐

    e.g. f = FiniteField(4, 19) → GF(2^4)을 primitive polynomial $x^4 + x + 1$ $(10011_{(2)} = 19)$를 사용하여 생성
  - printField 구현 : 오른쪽 그림과 같이 출력
  - 덧셈, 뺄셈, 곱셈, 나눗셈 구현
    - 입출력은 Finite Field의 원소, 만약 입력이 invalid한 경우에는 -1을 반환
  - GF(16)을 $x^4 + x + 1$ $(10011_{(2)} = 19)$로 생성했을 때의 연산 예시
    - add(3, 5) = 3(0011) + 5(0101) = 6 (0110)
    - sub(6, 3) = 6(0110) − 3(0011) = 5 (0101)
    - mul(2, 8) = 2(0010) × 8(1000) = α^1(0010) × α^3(1000) = α^4(0011) = 3 (0011)
    - mul(0, 4) = 0(0000) × 4(0100) = 0 (0000)
    - div(2, 3) = 2(0010) ÷ 3(0011) = α^1(0010) ÷ α^4(0011) = α^{12}(1111) = 15 (1111)

```
GF16 >>>>>>>>>>
      -inf 0000
         0 0001
         1 0010
         2 0100
         3 1000
         4 0011
         5 0110
         6 1100
         7 1011
         8 0101
         9 1010
        10 0111
        11 1110
        12 1111
        13 1101
        14 1001
```

Finite Field

- 제출 파일 : finitefield.py
- 제출 방법
  1. chmod o-rwx 이름.tar
  2. cp 이름.tar /home/ECC_ASSIGNMENTS/3rd/submit

```
f = FiniteField(4,19)

if f.success:
    f.printField()
    print('Add result is', f.add(3,5))
    print('Sub result is', f.sub(6,3))
    print('Mul result is', f.mul(2,8))
    print('Mul result is', f.mul(0,4))
    print('Div result is', f.div(2,3))

    print('Add result is ', f.add(3,16))
    print('Sub result is ', f.sub(-1,2))
    print('Mul result is ', f.mul(-1,55))
    print('Div result is ', f.div(5,0))
```

```
GF16 >>>>>>>>>>
      -inf 0000
         0 0001 1
         1 0010 2
         2 0100 4
         3 1000 8
         4 0011 3
         5 0110 6
         6 1100 12
         7 1011 11
         8 0101 5
         9 1010 10
        10 0111 7
        11 1110 14
        12 1111 15
        13 1101 13
        14 1001 9
```

```
Add result is 6
Sub result is 5
Mul result is 3
Mul result is 0
Div result is 15
Add result is  -1
Sub result is  -1
Mul result is  -1
Div result is  -1
```