ECC 3rd homework

Dongwhee Kim
Taewon Park

Finite Field

- Objective: Implement the `**FiniteField**` class
  - Inputs for class instantiation are `power` and `poly`
  - Only the creation of Finite Field GF(2^{power}) is considered, and `poly` is provided in decimal

    e.g. f = FiniteField(4, 19) → Creates GF(2^4) using the primitive polynomial ($x^4 + x + 1$)
    ($10011_2 = 19_{10}$)
  - Implement `**printField**`: Display as shown in the illustration on the right
  - Implement **addition, subtraction, multiplication, and division**
    - Inputs and outputs should be elements of the Finite Field. If the input is invalid, return -1
  - An **operation example** when GF(16) is created using ($x^4 + x + 1$) ($10011_2 = 19_{10}$)
    - 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

```python
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
```