0716221 余忠旻

1. Please write a program based on Berlekamp–Massey algorithm to find the shortest linear feedback shift register (LFSR) for the given sequence down below.

我根據 Berlekamp_Massey_algorithm 將它實作出來，
其中 f 用來存生成多項式的次項

```python
def Berlekamp_Massey_algorithm(sequence):
    N = len(sequence)
    s = sequence[:]

    for k in range(N):
        if s[k] == 1:
            break

    # use a set to denote polynomial
    f = set([k + 1, 0])
    l = k + 1

    g = set([0])
    a = k
    b = 0

    for n in range(k + 1, N):
        d = 0
        for ele in f:
            d ^= s[ele + n - l]

        if d == 0:
            b += 1
        else:
            if 2 * l > n:
                f ^= set([a - b + ele for ele in g])
                b += 1
            else:
                temp = f.copy()
                f = set([b - a + ele for ele in f]) ^ g
                l = n + 1 - l
                g = temp
                a = b
                b = n - l + 1
```

把剛才存的 f 轉成多項式印出來

```
    # output the polynomial
    result = ''
    lis = sorted(f, reverse=True)
    for i in lis:
        if i == 0:
            result += '1'
        else:
            result += 'x^%s' % str(i)

        if i != lis[-1]:
            result += ' + '

    return (result, l)
```

執行結果:

```
Its characteristic polynomial is (x^7 + x^1 + 1), and linear span is 7.
```

2. Find the sequence generation rule of 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610…….

   Generation rule is $a_{n+2} = a_{n+1} + a_n$, $a_0 = 0$, $a_1 = 1$

3. Use Berlekamp–Massey algorithm to find out the sequence rule of 0, 1, 1, 2, 3, 5, 8, 13, 21, 34

$s(x) = x^8 + x^7 + 2x^6 + 3x^5 + 5x^4 + 8x^3 + 13x^2 + 21x + 34$

$r(x) = x^9$

欲求次數小的c(x) 使得f(x)r(x) + c(x)s(x) = b(x)，deg b < deg c

算式	f(x)	c(x)	b(x)	
(1)	1	0	x^9	
(2)	0	1	$x^8 + x^7 + 2x^6 + 3x^5 + 5x^4 + 8x^3 + 13x^2 + 21x + 34$	
(3):(1)-(2)*(x-1)	1	$-x + 1$	$-x^7 - x^6 - 2x^5 - 3x^4 - 5x^3 - 8x^2 - 13x + 34$	
(4):(2)-(3)*(-x)	x	$-x^2 + x + 1$(答案)	$55x + 34$	（完成）