1. Write a program based on Berlekamp–Massey algorithm to find the shortest linear feedback shift register (LFSR).

首先對 input 做處理，存進 seq 中，再放入 Berlekamp_Massey 的 func。

```
seq = re.sub(r"[^01]", "", input("Input sequence = "))
(poly, span) = Berlekamp_Massey_algorithm(seq)
```

```
Input sequence = 1,0,0,1,0,0,0,0,1,1,1,1,0,1,0,0,0,0,1,1,1,0,0,0,0,0,0,1,1
10010000111101000011100000011
[1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1]
```

跑 for 迴圈找出 seq 的前 k+1 位的最低次多項式，並用變數 l 存起來。
f 為使用集合来表示多項式，之後計算當前(n)的 d 值。

```
def Berlekamp_Massey(sequence):
    N = len(sequence)
    seq = [int(i) for i in sequence]

    for k in range(N):
        if seq[k] == 1:
            break
    f = set([k + 1, 0])
    l = k + 1
```

$$d = s_N \oplus \sum_{i=0}^{m-1} c_i s_{N-1-i}$$

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

若 d = 0，即能生成 seq 的前 n+1 項的最低次多項式，而 d = 1，則不能生成。
判斷後將集合 f 做 n 次 Euclidean algorithm 以求得結果。

```
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
```

如下圖輸入 4 個 sequence 所示，此部分 code 為最後輸出多項式。

```python
def print_poly(polynomial):
    result = ''
    lis = sorted(polynomial, reverse=True)
    for i in lis:
        if i == 0:
            result += '1'
        else:
            result += 'x^%s' % str(i)

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

```
PS C:\Users\JasmineLu\Downloads\github> & C:/Users/JasmineLu/AppData/Local/Microsoft/WindowsApps/python3.8.exe
c:/Users/JasmineLu/Downloads/github/NYCU_Cryptography-Engineering/Quiz7/310555004.py
Input sequence = 10010000111101000011100000011
Characteristic polynomial is (x^14 + x^13 + x^12 + x^11 + x^9 + x^8 + x^6 + x^5 + x^3 + x^2 + 1)
Input sequence = 00001110110101000110111100011
Characteristic polynomial is (x^16 + x^13 + x^11 + x^10 + x^8 + x^7 + x^4 + x^3 + x^2 + 1)
Input sequence = 10101111010001001010111100010
Characteristic polynomial is (x^15 + x^13 + x^12 + x^10 + x^7 + x^5 + x^4 + x^3 + x^1)
Input sequence = 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0
, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0
, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1
Characteristic polynomial is (x^7 + x^1 + 1)
```

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

A: 此數列為費波那契數列

$a_{n+2} = a_{n+1} + a_n$

$a_0 = 0$

$a_1 = 1$

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

A: $x^2 + x$