

Q1

程式碼邏輯：

我使用了galois這個module，讓他幫我處理在輾轉相除法時會用到的 $+$ - $*$ 。

首先讀取輸入字串，我預設輸入字串都由 $\{0, 1\}$ 組成，字串的長度為2的倍數。接著把輸入字串轉成galois中的polynomial且定義在 $GF(2)$ 底下，再來照著投影片的方法去算輾轉相除法，在 $B(x) > GCD$ 的時候停止輾轉相除法，此時的 $B(x)$ 即為modified Berlekamp-Massey algorithm的答案，再將答案用polynomial的形式輸出出來。

下面這個問題我有在github詢問助教了：

我有一個不清楚的地方是為什麼input長度一定要是2的倍數才可以算出正確答案？

我在這篇論文有看到類似的演算法，他同樣假設input長度是2的倍數。<http://hlombardi.free.fr/publics/BMAvar.pdf>

注意到的事情：

1.算的時候好像可以直接用 $quotient = gcd1 // gcd2$ ，不用和投影片一樣一次算一位，目前測試下來兩種方式答案都一樣，但我還是照投影片的方式

2.看投影片好像是說gcd1比gcd2小時改成gcd2去除gcd1，但不知道為什麼處理這個情況後反而會錯，不知道是有寫錯還是其實不用這樣做或是有其他問題 e.g.quiz7 q1的input，所以我就沒有處理這個情況

Q2

是fibonacci sequence，他的遞迴式是 $a_0 = 0, a_1 = 1, a_{n+2} = a_n + a_{n+1}$, for $n \in \text{正整數 union } \{0\}$ ，也就是前兩項和=下一項。

Q3

(在下一頁)

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

$$r(x) = x^9$$

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

列表 算式	f(x)	c(x)	b(x)						
(1)	1	0	x^9						
(2)	0	1	$x^8+x^7+2x^6+3x^5+5x^4+8x^3+13x^2+21x+34$						
X	1	-X	$-x^8-2x^7-3x^6-5x^5-8x^4-13x^3-21x^2-34x$						
-1	1	-x+1	$-x^7-x^6-2x^5-3x^4-5x^3-8x^2-13x+34$						
X	-x+1	x^2-2x	$-x^7-x^6-2x^5-3x^4-5x^3-8x^2-68x$						
1	X	$-x^2+x+1$	$> 55x+34$						
$\Rightarrow C(x) = -x^2+x+1$									
			\neq						