$$\overset{a(x)}{(x^5+x^4+x^3+x^2)} \cdot \overset{b(x)}{(x^5+x^2+x+1)}$$

$$= x^{10}+x^7+x^6+x^5+x^9+x^6+x^5+x^4+x^8+x^5 + x^4+x^3+x^7+x^4+x^3+x^2$$

$$= x^{10}+x^9+x^8+x^5+x^4+x^2$$

$$\begin{array}{l|l} x^{10}+x^9+x^8+x^5+x^4+x^2 & x^8+x^4+x^3+x+1 \\ \cline{2-2} x^{10}+x^6+x^5+x^3+x^2 & x^2+x+1 \\ \hline x^9+x^8+x^6+x^4+x^3 & \\ x^9+x^5+x^4+x^2+x & \\ \hline x^8+x^6+x^5+x^3+x^2+x & \\ x^8+x^4+x^3+x+1 & \\ \hline x^6+x^5+x^4+x^2+1 & \end{array}$$

$a(x) \cdot b(x) \bmod m(x) = x^6+x^5+x^4+x^2+1$

Input : 2 mảng A[ ], B[ ], lưu số mũ 2 đa thức
mảng M[ ] lưu số mũ m(x)

B_1: Tạo mảng mul[ ] để lưu số mũ ~~x~~ khi nhân 2 mảng A, B

B_2:

Lặp qua từng phần tử của mảng A. Với mỗi phần tử đó ~~nhân~~ với từng phần tử mảng B.

Nếu khi cộng phần kiểm tra trong mul[ ] đã tồn tại thì remove nó

```
for i in A :
    for j in B :
        if (i + j) not in mul :
            mul.append(i + j)
        else : mul.pop(i + j)
```

B_3: Tạo mảng mod[ ] để lưu kết quả khi chia dư

B_4: Sắp xếp mảng mul theo thứ tự giảm dần

Lặp cho tới khi mul[0] < M[0] :

+ Tạo biến tmp = mul[0] - M[0]
+ ~~Nhâ~~ Cộng tmp vs từng phần tử M[ ] rồi lưu vào mod[ ]
+ Lặp qua từng phần tử mod[ ] nếu trong mul[ ] có thì xoá phần tử đó và ngc lại trong mul[ ]
+ Sắp xếp lại mul[ ] giảm dần
+ Xoá hết phần tử trong mod[ ]

Chạy ví dụ

Thứ...... Ngày....... ....

A = [5, 4, 3, 2]

B = [5, 2, 1, 0]

M = [8, 4, 3, 1, 0]

[5, 4, 3, 2]

[5, 2, 1, 0]

Mul = [10, $\cancel{7}$, $\cancel{6}$, $\cancel{5}$, 9, $\cancel{6}$ $\cancel{5}$, $\cancel{4}$, 8, 5, $\cancel{4}$, $\cancel{3}$, $\cancel{7}$, 4, $\cancel{3}$, 2]

= [10, 9, 8, 5, 4, 2]

10, 9, 8, 5, 4, 2	8, 4, 3, 1, 0
10, 6, 5, 3, 2	2, 1, 0
9, 8, 6, 4, 3	
9, 5, 4, 2, 1	
8, 6, 5, 3, 2, 1	
8, 4, 3, 1, 0	
6, 5, 4, 2, 0	

Mul = [6, 5, 4, 2, 0]

$$x^6 + x^5 + x^4 + x^2 + 1$$