ADSP 補充教材

張國韋 Kuo-Wei Chang [1]

[1]Chunghwa Telecom

May 24 2023

國立臺灣大學 National Taiwan University 中華電信研究院 Chunghwa Telecom Laboratories

Table of contents I

Section 1

如何求出 primitive root

其實没有好方法

- wiki 百科連結

Section 2

如何求出 $g^n \mod M$

兩招

- 建表來查
- 平方法，可對任何數通用

平方法

假設我們要算 $3^{32} \mod 101$

- 首先先算 $3^2 = 9, 9^2 = 81$

平方法

假設我們要算 $3^{32} \mod 101$

- 首先先算 $3^2 = 9, 9^2 = 81$
- 然後算 $3^8 = 81^2 = 6561 = 97 \mod 101$

平方法

假設我們要算 $3^{32} \mod 101$

- 首先先算 $3^2 = 9, 9^2 = 81$
- 然後算 $3^8 = 81^2 = 6561 = 97 \mod 101$
- 接下來 $3^{16} = 97^2 = 9409 = 16 \mod 101$

平方法

假設我們要算 $3^{32} \mod 101$

- 首先先算 $3^2 = 9, 9^2 = 81$
- 然後算 $3^8 = 81^2 = 6561 = 97 \mod 101$
- 接下來 $3^{16} = 97^2 = 9409 = 16 \mod 101$
- 最後 $3^{32} = 16^2 = 256 = 54 \mod 101$

如果不是 32 次方怎麼辦呢

大家可以先想想看

變成 2 進位

- 令 $t = 1$，從最左邊開始
- 如果遇到 1，就 $t = t^2 \cdot g$
- 如果遇到 0，就 $t = t^2$

例子

計算 $3^{10} \mod 101$

1. 10=1010
2. t=1，看到最左邊的 1，變成 3
3. 然後看到 0，變成 9
4. 然後又看到 1，變成 $9^2 \cdot 3 = 243 = 41 \mod 101$
5. 最後看到 0，變成 $41^2 = 1681 = 65 \mod 101$

Section 3

如何求出 $g^{-1} \mod M$

輾轉相除法

- 其實對所有數字都可以用來求它的 inverse
- 也就是求最大公因數啦
- 可能有同學已經聽過，但還是來玩玩看吧

請求出 47 在 101 的 inverse

1. $101 = 47 \times 2 + 7$
2. $47 = 7 \times 6 + 5$
3. $7 = 5 + 2$
4. $5 = 2 \times 2 + 1$

然後呢

1. $5 - 2 \times 2 = 1, \because 5 = 2 \times 2 + 1$
2. $5 - (7 - 5) \times 2 = 1, \because 7 = 5 + 2$
3. $5 \times 3 - 7 \times 2 = 1$
4. $(47 - 7 \times 6) \times 3 - 7 \times 2 = 1, \because 47 = 7 \times 6 + 5$
5. $47 \times 3 - 7 \times 20 = 1$
6. $47 \times 3 - (101 - 47 \times 2) \times 20 = 1, \because 101 = 47 \times 2 + 7$
7. $47 \times 43 - 101 \times 20 = 1$ **答案 43 即爲所求**

Matlab: [d,u,v]=gcd(a,b)
d=u*a+v*b

Section 4

把 DFT 和 NTT 延伸到 finite field 吧

What is a finite field

先假裝大家都知道吧
課後記得去讀 Galois 的生平

- wolfram 連結

問問大家

- 大家覺得 NTT 和 DFT 裏面最相似的東西是什麼呢？

問問大家

- 大家覺得 NTT 和 DFT 裏面最相似的東西是什麼呢？
- 另個問法，大家覺得爲何 NTT 會垂直呢？

秘密

$g^N = 1 \mod M$. Let

$$S = \sum_{k=0}^{N-1} g^k \tag{1}$$

$$gS = g \sum_{k=0}^{N-1} g^k \tag{2}$$

$$= \sum_{k=1}^{N} g^k = \sum_{k=1}^{N-1} g^k + g^N = S \tag{3}$$

since $g^N = g^0 = 1$. If $g \neq 1$ we have $S = 0$.

所以我們看看

Consider $GF(2^4)$, primitive polynomial:$x^4 + x + 1$
總共有 16 個元素，

0	1	x	x^2
x^3	$x^4 = x + 1$	$x^5 = x^2 + x$	$x^6 = x^3 + x^2$
$x^7 = x^3 + x + 1$	$x^8 = x^2 + 1$	$x^9 = x^3 + x$	$x^{10} = x^2 + x + 1$
$x^{11} = x^3 + x^2 + x$	$x^{12} = x^3 + x^2 + x + 1$	$x^{13} = x^3 + x^2 + 1$	$x^{14} = x^3 + 1$

注意：$x^{15} = xx^{14} = x^4 + x = (x + 1) + x = 1$
也就是我們可以做 3 點或 5 點的 Finite field transform 來玩

比如三點

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & x^5 & x^{10} \\ 1 & x^{10} & x^5 \end{bmatrix}$$

注意：上一頁說 $x^5 = x^2 + x,\ x^{10} = x^2 + x + 1$
剛好驗證 $1 + x^5 + x^{10} = 0$

結論

- 只要 $g^N = 1$, 就能做出 N-point transform
- 性質都會跟 DFT 一樣

Section 5

還有哪些性質跟 DFT 一樣

例子 1 Inpulse train

方便起見，還是回到 NTT(剛剛那個 GF 真的很難算) Let $M = 13, N = 6$

$$F = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 3 & 12 & 9 & 10 \\ 1 & 3 & 9 & 1 & 3 & 9 \\ 1 & 12 & 1 & 12 & 1 & 12 \\ 1 & 9 & 3 & 1 & 9 & 3 \\ 1 & 10 & 9 & 12 & 3 & 4 \end{bmatrix}, x = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, y = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

比較一下，Fx 和 fft(x) 有何相似，Fy 和 fft(y) 呢？

例子 2 Legendre sequence

Let $M = 11, N = 5$

$$F = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 5 & 9 & 3 \\ 1 & 5 & 3 & 4 & 9 \\ 1 & 9 & 4 & 3 & 5 \\ 1 & 3 & 9 & 5 & 4 \end{bmatrix}, x = \begin{bmatrix} 0 \\ 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}$$

比較一下，Fx 和 fft(x) 有何相似

最後

希望大家有學到東西，有緣再見！