

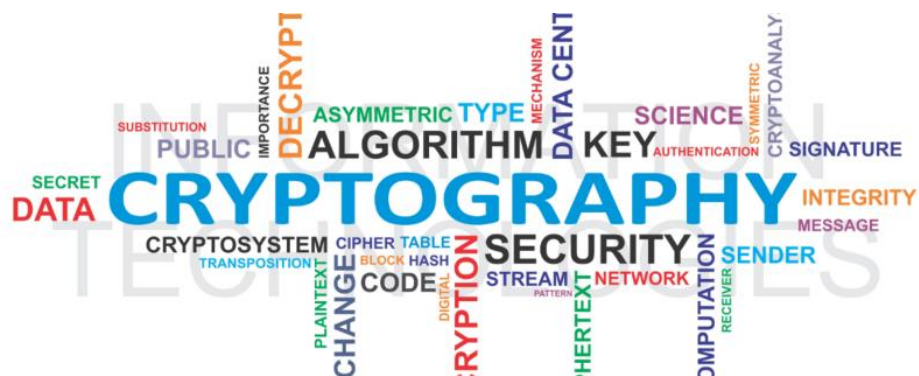
Chương 2

CƠ SỞ TOÁN HỌC

Mathematic Foundation

PGS.TS. Lê Đức Như

✉ Nhuongld@hus.edu.vn ☎ 0987.394.900.



Nội dung chương 2

2.1 Lý thuyết số học đồng dư

2.2 Phần tử nghịch đảo

2.3 Bài toán Logarit rời rạc

2.4 Kiểm tra số nguyên tố

2.5 Bài toán phân tích số nguyên tố

2.6 Hàm một phía và hàm cửa sập một phía

2.7 Lý thuyết về độ phức tạp tính toán

2.1 Lý thuyết số học đồng dư



► Đồng dư modulo

- ▶ Giả sử a và b là các số nguyên và m là một số nguyên dương.
- ▶ Khi đó ta viết $a \equiv b \pmod{m}$ nếu m chia hết cho $b-a$.
- ▶ Mệnh đề $a \equiv b \pmod{m}$ được gọi là “ a đồng dư với b theo modun m ”

- ▶ Giả sử:

$$a = q_1 * m + r_1 \text{ và } b = q_2 * m + r_2$$

trong đó $0 \leq r_1 \leq m-1$ và $0 \leq r_2 \leq m-1$.

- ▶ Khi đó có thể dễ dàng thấy rằng:

$$a \equiv b \pmod{m} \text{ khi và chỉ khi } r_1 = r_2$$

2.1 Lý thuyết số học đồng dư

- ▶ Ký hiệu **$a \bmod m$** để xác định phần dư khi a được chia cho m .
- ▶ Như vậy: **$a \equiv b \pmod{m}$** khi và chỉ khi:

$$(a \bmod m) = (b \bmod m).$$

- ▶ Thay giá trị **a** bằng **$(a \bmod m)$** tức là **a được rút gọn theo modulo m** .
 - Nhiều ngôn ngữ lập trình: **$a \bmod m$** là phần dư trong dải **$-m+1, \dots, m-1$** có cùng dấu với **a** . Ví dụ **$-18 \bmod 7 = -4$** , giá trị này khác với giá trị 3 là giá trị được xác định theo công thức trên (vì phần bù: **$7 - 4 = 3$**)
 - Quy ước: **$a \bmod m$ luôn là một số không âm**

2.1 Lý thuyết số học đồng dư

► Số học modun m:

- Z_m là tập hợp $\{0, 1, \dots, m-1\}$ có trang bị hai phép toán cộng và nhân.
- Việc cộng và nhân trong Z_m được thực hiện giống như cộng và nhân các số thực ngoại trừ một điểm là các kết quả được rút gọn theo modun m.

► Ví dụ:

- Z_{26} là tập hợp $\{0, 1, 2, \dots, 25\}$ có trang bị hai phép toán cộng và nhân.
- $25 + 7 = 32 \bmod 26 = 6$ (ví dụ K=7, 'Z' \rightarrow 'H')
- $5 * 9 = 45 \bmod 26 = 19$

2.1 Lý thuyết số học đồng dư

► Định lý về đồng dư thức

- Đồng dư thức $ax \equiv b \pmod{m}$ chỉ có một nghiệm duy nhất $x \in \mathbb{Z}_m$ với mọi $b \in \mathbb{Z}_m$ khi và chỉ khi $\text{UCLN}(a, m) = 1$.

► Ví dụ 1: $a=7, b=5, m=11$

- Đồng dư thức $7x \equiv 5 \pmod{11}$, kiểm tra: $\text{UCLN}(7, 11) = 1$
 - Có một nghiệm duy nhất $x=7$ vì $7 \cdot 7 \bmod 11 = 49 \bmod 11 = 5$
- Để giải phương trình đồng dư thức áp dụng công thức sau:

$$7x - 5 \text{ phải chia hết cho } 11$$

► Ví dụ 2: giải phương trình $5x \equiv 7 \pmod{11}$

- KQ $x=8$

2.2 Phần tử nghịch đảo

▶ Khái niệm phần tử nghịch đảo

- ▶ Giả sử $a \in \mathbb{Z}_m$.
- ▶ Phần tử nghịch đảo của a là phần tử $a^{-1} \in \mathbb{Z}_m$ sao cho:

$$aa^{-1} \equiv a^{-1}a \equiv 1 \pmod{m}$$

▶ Tính chất

- ▶ a có nghịch đảo theo môđun m khi và chỉ khi $\text{UCLN}(a, m) = 1$,
- ▶ Nếu nghịch đảo tồn tại thì phải là duy nhất.
- ▶ Nếu $b = a^{-1}$ thì $a = b^{-1}$.
- ▶ Nếu m là số nguyên tố thì mọi phần tử khác không của \mathbb{Z}_m đều có nghịch đảo.

2.2 Phần tử nghịch đảo

▶ Thuật toán Euclide tìm ước chung lớn nhất của 2 số a, n

▶ Ký hiệu

(a, n) là ước số chung lớn nhất của a, n ; Giả sử $n > a$.

$\phi(n)$ là số các số nguyên dương $< n$ và nguyên tố với n .

Thuật toán Euclide tìm UCLN (a, n) được thực hiện:

▶ Đặt $r_0 = n, r_1 = a,$

▶ $r_0 = q_1 r_1 + r_2, \quad 0 < r_2 < r_1$

▶ $r_1 = q_2 r_2 + r_3, \quad 0 < r_3 < r_2$

▶

▶ $r_{m-2} = q_{m-1} r_{m-1} + r_m, \quad 0 < r_m < r_{m-1}$

▶ $r_{m-1} = q_m r_m$

▶ Thuật toán phải kết thúc ở một bước thứ m nào đó. Ta có:

$$(n, a) = (r_0, r_1) = (r_1, r_2) = \dots = (r_{m-1}, r_m) = r_m$$

2.2 Phần tử nghịch đảo



- ▶ **Thuật toán Euclide mở rộng tìm phần tử nghịch đảo**
- ▶ Ta tìm được $r_m = (n, a)$. Mở rộng thuật toán Euclide bằng cách xác định thêm dãy số t_0, t_1, \dots, t_m :
 - ▶ $t_0 = 0, t_1 = 1,$
 - ▶ **$t_j = t_{j-2} - q_{j-1}t_{j-1} \bmod r_0$, nếu $j \geq 2$,**

2.2 Phần tử nghịch đảo

Thuật toán Euclide mở rộng tìm phần tử nghịch đảo

- **Bước 1**: Xây dựng bảng (gồm 6 cột) như sau:

Dòng	r_0	r_1	r_2	q	t_0	t_1

Trên mỗi dòng, ta có: $r_0 = r_1 \times q + r_2$

- **Bước 2**: Điền giá trị vào dòng đầu tiên $r_0 = n$, $r_1 = a$, $t_0 = 0$, $t_1 = 1$

Dòng	r_0	r_1	r_2	q	t_0	t_1
0	n	a			0	1

2.2 Phần tử nghịch đảo

- **Bước 3:** Trên dòng i đang xét, tính giá trị

$$r_2 = r_0 \bmod r_1,$$

$$q = \lfloor r_0 / r_1 \rfloor$$

Dòng	r_0	r_1	r_2	q	t_0	t_1
...
i			$r_0 \bmod r_1$	$\lfloor r_0 / r_1 \rfloor$		

- **Bước 4:** Tính giá trị t_1 (của dòng i) từ giá trị q , t_0 và t_1 của dòng $i-1$.

Dòng	r_0	r_1	r_2	q	t_0	t_1
...
$i-1$				X	Y	Z
i						$Y - X \times Z \bmod n$

2.2 Phần tử nghịch đảo

► **Bước 5:** Trên dòng i đang xét:

► **Nếu** $r_2 = 0$ **thì**:

► **Nếu** $r_1 = 1$ **thì** giá trị t_1 là phần tử nghịch đảo của a trong Z_n

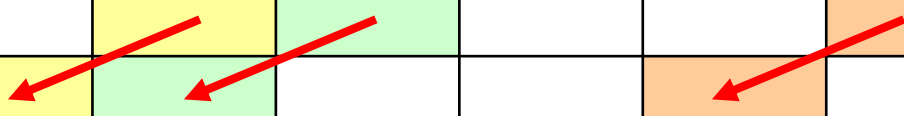
► **Ngược lại** (tức là $r_1 \neq 1$) **thì** không tồn tại phần tử nghịch đảo. Dừng

► **Ngược lại** (tức là $r_2 \neq 0$) thì sang bước 6

Dòng	R_0	r_1	r_2	q	t_0	t_1
...
i		$r_1 = 1?$	$r_2 = 0?$			

► **Bước 6:** Sao chép giá trị sang dòng tiếp theo theo quy tắc dưới đây, sau đó, trở lại **bước 3**:

Dòng	r_0	r_1	r_2	q	t_0	t_1
i						



2.2 Phần tử nghịch đảo

□ Ví dụ 1: $n=101$, $a = 25$

Dòng	r_0	r_1	r_2	q	t_0	t_1
0	101	25	1	4	0	1

Dòng	r_0	r_1	r_2	q	t_0	t_1
0	101	25	1	4	0	1
1	25	<u>1</u>	<u>0</u>	25	1	<u>97</u>

Vậy $25^{-1} = 97$ (trong Z_{101})

□ Ví dụ 2: $n = 1024$, $a = 173$

Dòng	r_0	r_1	r_2	q	t_0	t_1
0	1024	173	159	5	0	1
1	173	159	14	1	1	1019
2	159	14	5	11	1019	6
3	14	5	4	2	6	953
4	5	4	1	1	953	148
5	4	<u>1</u>	<u>0</u>	4	148	<u>805</u>

Vậy $173^{-1} = 805$ (trong Z_{1024})

2.3 Bài toán Logarit rời rạc

► Discrete Logarithmic Problem (DLP)

- Thiết lập môi trường hữu hạn $\mathbf{Z_p}$, p là số nguyên tố.
- Nhóm Cyclic $\mathbf{Z_p^*}$ và phần tử sinh (phần tử nguyên thủy)
- Đặc trưng của bài toán: $\mathbf{I = (p, \alpha, \beta)}$ trong đó p là số nguyên tố, $\alpha \in \mathbf{Z_p}$ là phần tử nguyên thủy, $\beta \in \mathbf{Z_p^*}$
- Mục tiêu: Hãy tìm một số nguyên duy nhất a , $0 \leq a \leq p-2$ sao cho:

$$\alpha^a \equiv \beta \pmod{p}$$

Ta sẽ xác định số nguyên:

$$a = \log_{\alpha} \beta \pmod{p}$$

2.4 Kiểm tra số nguyên tố



- ▶ Số nguyên dương $p > 1$ là *nguyên tố* nếu p không chia hết cho số nguyên dương nào ngoài 1 và p .

```
1.int ktra(int a)
2.{
3.    int i,dem=0;
4.    for(i=1;i<=a[i];i++)
5.        if(a[i]%i==0) dem++;
6.    return (dem==2)? 1: 0;
7.}
```

- ▶ Dự án Sierpinski đã tìm ra được số nguyên tố khổng lồ là số $10.223 * 2^{31172165} + 1$, dài **9.383.761 chữ số**.
- ▶ Một chiếc máy tính thông thường sẽ phải mất nhiều thế kỷ để có tìm ra con số khổng lồ này. Kết quả dài hơn 9 triệu chữ số kia là sản phẩm của hàng nghìn chiếc máy tính chạy liên tục trong 8 ngày.

2.4 Kiểm tra số nguyên tố

- ▶ Số nguyên tố lớn nhất (2016): chiều dài của nó lên tới **22 triệu chữ số** ($2^{74.207.281} - 1$) được in ra 3 quyển sách.



- ▶ Số nguyên tố lớn nhất (2018) đặt tên M77232917 có giá trị bằng **$2^{77.232.917} - 1$** , cho ra một dãy số khổng lồ có **23.249.425 chữ số**. M77232917 có thể được biểu diễn trên 9.000 trang giấy, kéo dài 118km với độ dài 1 chữ số là 0,5cm.

2.4 Kiểm tra số nguyên tố



Giải thuật kiểm tra Miller-Rabin

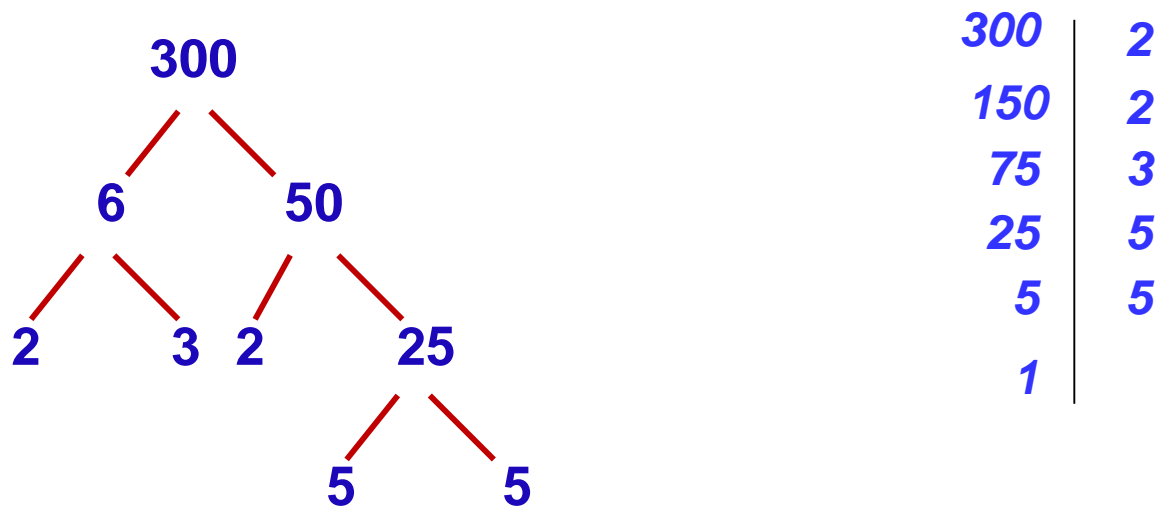
INPUT Số tự nhiên lẻ n .

OUTPUT NguyênTo: TRUE/FALSE

1. Phân tích $n - 1 = 2^s \cdot m$ trong đó $s \geq 1$ và m là số tự nhiên lẻ
2. Chọn ngẫu nhiên số tự nhiên $a \in \{2, \dots, n-1\}$.
3. Đặt $b = a^m \pmod{n}$
4. Nếu $b \equiv -1 \pmod{n}$ thì trả về TRUE. Kết thúc.
5. Cho k chạy từ 0 đến s :
 1. Nếu $b \equiv -1 \pmod{n}$ thì trả về TRUE. Kết thúc.
 2. Thay $b := b^2 \pmod{n}$.
6. Trả lời FALSE. Kết thúc.

2.5 Phân tích ra thừa số nguyên tố

- Phân tích một số tự nhiên lớn hơn 1 ra thừa số nguyên tố là viết số đó dưới dạng một tích các thừa số nguyên tố.



$$300 = 2 \cdot 3 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 3 \cdot 5^2$$

2.6 Hàm 1 phía và hàm cửa sập 1 phía DUY TÂN UNIVERSITY

▶ Hàm một phía

- ▶ Hàm $f(x)$ được gọi là hàm một phía, nếu:

▶ Tính $y = f(x)$ là dễ, nhưng tính ngược $x = f^{-1}(y)$ là rất khó.

- ▶ Ví dụ: Hàm $f(x) = g^x \pmod{p}$ (p là số nguyên tố, g là phần tử nguyên thủy theo modun p) là hàm một phía.
 - ▶ Biết x tính $f(x)$ là khá đơn giản
 - ▶ Biết $f(x)$ để tính x thì với các thuật toán đã biết hiện nay đòi hỏi một khối lượng tính toán cỡ lớn (với máy tính mạnh nhất mất khoảng 3000 năm)

2.6 Hàm 1 phía và hàm cửa sập 1 phía

▶ Hàm cửa sập một phía

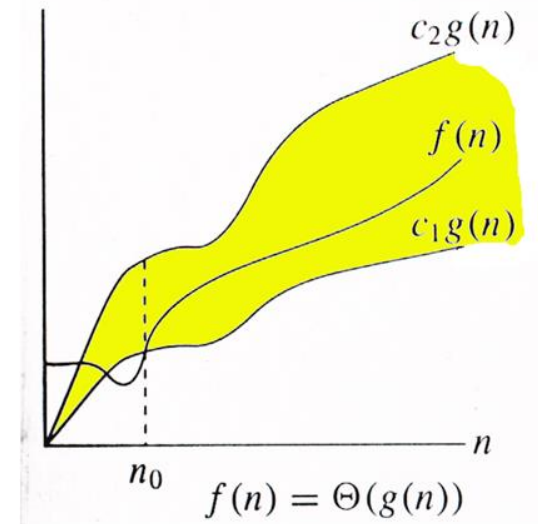
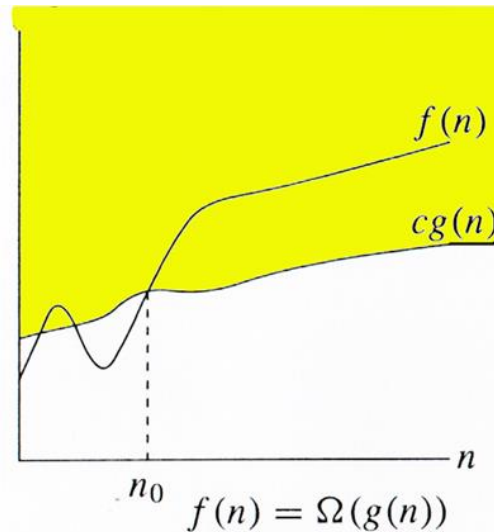
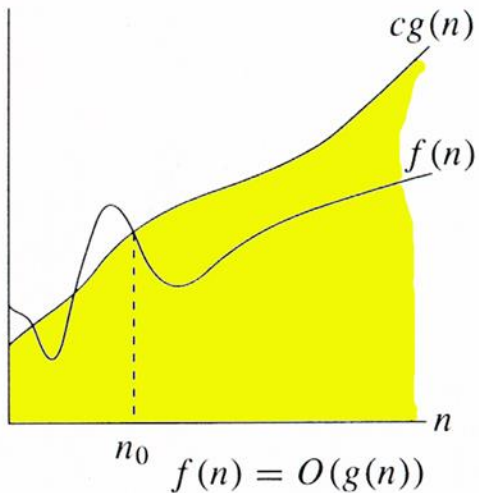
- ▶ Hàm $f(x)$ được gọi là hàm cửa sập một phía, nếu:

- ▶ Tính $y = f(x)$ là dễ, tính $x = f^{-1}(y)$ là rất khó
- ▶ Nhưng có cửa sập z để tính $x = f_z^{-1}(y)$ là dễ

- ▶ Ví dụ: $n = p \times q$ là tích của hai số nguyên tố lớn, a là số nguyên, hàm $f(x) = x^a \pmod n$ là hàm cửa sập một phía.

- ▶ Nếu chỉ biết n và a thì tính $x = f^{-1}(y)$ là rất khó,
- ▶ Nếu biết cửa sập, chẳng hạn hai thừa số của n , thì sẽ tính được $f^{-1}(y)$ khá dễ

2.7 Lý thuyết về độ phức tạp tính toán

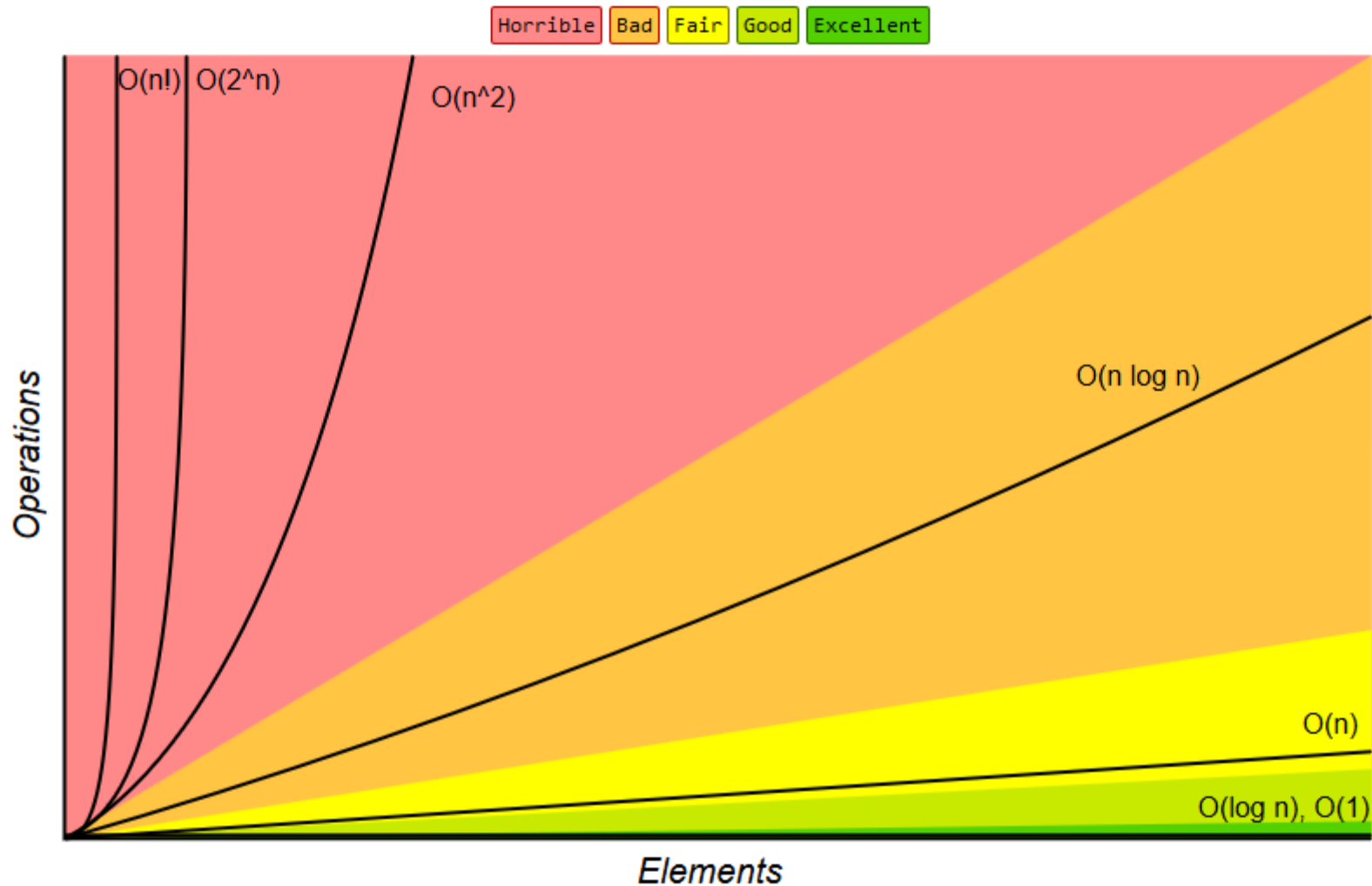


2.7 Lý thuyết về độ phức tạp tính toán

Algorithm	Time Complexity			Space Complexity
	Best	Average	Worst	Worst
<u>Quicksort</u>	$\Omega(n \log(n))$	$\Theta(n \log(n))$	$O(n^2)$	$O(\log(n))$
<u>Mergesort</u>	$\Omega(n \log(n))$	$\Theta(n \log(n))$	$O(n \log(n))$	$O(n)$
<u>Timsort</u>	$\Omega(n)$	$\Theta(n \log(n))$	$O(n \log(n))$	$O(n)$
<u>Heapsort</u>	$\Omega(n \log(n))$	$\Theta(n \log(n))$	$O(n \log(n))$	$O(1)$
<u>Bubble Sort</u>	$\Omega(n)$	$\Theta(n^2)$	$O(n^2)$	$O(1)$
<u>Insertion Sort</u>	$\Omega(n)$	$\Theta(n^2)$	$O(n^2)$	$O(1)$
<u>Selection Sort</u>	$\Omega(n^2)$	$\Theta(n^2)$	$O(n^2)$	$O(1)$
<u>Tree Sort</u>	$\Omega(n \log(n))$	$\Theta(n \log(n))$	$O(n^2)$	$O(n)$
<u>Shell Sort</u>	$\Omega(n \log(n))$	$\Theta(n(\log(n))^2)$	$O(n(\log(n))^2)$	$O(1)$
<u>Bucket Sort</u>	$\Omega(n+k)$	$\Theta(n+k)$	$O(n^2)$	$O(n)$
<u>Radix Sort</u>	$\Omega(nk)$	$\Theta(nk)$	$O(nk)$	$O(n+k)$
<u>Counting Sort</u>	$\Omega(n+k)$	$\Theta(n+k)$	$O(n+k)$	$O(k)$
<u>Cubesort</u>	$\Omega(n)$	$\Theta(n \log(n))$	$O(n \log(n))$	$O(n)$

2.7 Lý thuyết về độ phức tạp tính toán

Big-O Complexity Chart



2.7 Lý thuyết về độ phức tạp tính toán

