# Estufa en Piloto



## Contents

1	$\mathbf{Bas}$	ic	<b>2</b>					
	1.1	Binary Search	2					
	1.2	LIS	2					
		1.2.1 Naive	2					
		1.2.2 Fast	2					
<b>2</b>	Data Structures 3							
	2.1	DSU	3					
	2.2	FenwickTree	4					
	2.3	Segment Tree	5					
	2.4	Sparse Table	6					
3	Graph 7							
	3.1	BFS	7					
	3.2	DFS	7					
	3.3	Dijkstra	8					
	3.4	Floyd-Warshall	8					
	3.5	Max Flow-Min Cut (Ford Fulkerson)	8					
4	Math 10							
	4.1	Identities	10					
	4.2	GCD	10					
	4.3	Euler Totient (Phi)	10					

	4.4	Extended Euclides	0
	4.5	Modexp	0
	4.6	allModInv	0
	4.7	Iter multiplication	1
	4.8	Test de primalidad y Descomposicion en Primos	1
		4.8.1 Is Prime	1
		4.8.2 Miller Rabin Test	1
		4.8.3 Prime Factors	2
		4.8.4 Integer Fact	3
	4.9	Diofanticas	5
	4.10	Cribas	6
		4.10.1 Criba Primos	6
		4.10.2 Block Sieving	6
		4.10.3 Linear Sieve	7
	4.11	Divisores	7
		4.11.1 Count Divisors	
		4.11.2 Suma Divisores	
	4.12	Factorial	8
		4.12.1 Factorial mod	8
		4.12.2 Factorial Divisors	8
	4.13	FFT	
		Lagrange Interpolation	0
		Discrete Log	
		Discrete Root	
		Primitive Root	
		Fibonacci	1
		Gray Code	2
		Matrix	2
5	Geo	2c	3
	5.1	Convex Hull	3
	5.2	Determinant	3
	5.3	GreatCircleDistance	3
	5.4	Perimeter	3
	5.5	Turn	3
6	Stri	ngs 2	1
U	6.1	Hash	_
	6.2	Prefix Function	_
	6.2	KMP	
	6.4		_
	6.5	Rabin Karp	-
	6.6	ı v	о 6

Notebook Python 1 B.		ASIC - Page		
6.7 Group Identical Strings	26	1 Basic		
7 Tricks With Bits	27	1.1 Binary Search		
8 Plantilla		<pre>def _binsearch(lista, x, 1 , r):     """Recursive binsearch between 1 and r index in lista"""     #Couldn't find x in lista     if(r&lt;1): return -1     mid = (l+r)//2     if(lista[mid] == x): return mid     return _binsearch(lista, x, 1 , mid-1) if(x<lista[mid]) """wrapper="" ,="" 0="" _binsearch(l,="" _binsearch(lista,="" binsearch"""="" binsearch(l,="" def="" element="" element):="" else="" len(l)-1)<="" mid+1,="" of="" pre="" r)="" recursive="" return="" x,=""></lista[mid])></pre>		
		1.2 LIS		
		1.2.1 Naive		
		<pre>def LIS(1):     """Return the lenght of Longest Increasing Subsequence in 1"""     dp = [1 for _ in range(len(1))] #dp[i]: lenght of LIS containing 1[</pre>		
		<pre>from bisect import bisect_right import heapq def find_gt(a, x):  'Find_leftmost_value_greater_than_x' i = bisect_right(a, x) return i if i != len(a) else -1</pre>		

```
def LIS(arr):
       piles = []
9
10
       for idx in range(len(arr)):
11
           aux = [piles[i][-1] for i in range(len(piles))]
12
           pileNumber = find_gt(aux,arr[idx])
13
           if(pileNumber==-1):
14
               piles.append([arr[idx]])
15
           else:
16
               piles[pileNumber].append(arr[idx])
17
18
       print(piles)
19
       aux = [piles[i][::-1] for i in range(len(piles))]
20
       orden = list(heapq.merge(*aux))
21
       print(orden)
22
```

## 2 Data Structures

#### 2.1 DSU

```
class DisjointSetUnion:
       def __init__(self, array):
           self.parent = [i for i in array]
3
           self.rank = [0 for _ in range(len(array))]
4
           self.size = [1] * (len(array) + 1)
           self.group = [[a[i]] for i in array]
6
       def find(self, x):
8
           # If x is root
           if self.parent[x] == x:
10
                return x
11
           # If x is not root, search again by using x's parent
12
13
               self.parent[x] = self.find(self.parent[x])
14
                return self.parent[x]
15
16
       def union(self, x, y):
17
           x = self.find(x)
18
           y = self.find(y)
19
           # Make an edge from the root of lower tree to the root of higher
20
           if self.rank[x] < self.rank[y]:</pre>
21
               self.parent[x] = y
22
                self.size[y] += self.size[x]
23
           else:
24
               self.parent[y] = x
25
               self.size[x] += self.size[y]
26
                # If the height of tree the tree is the same, increase one
27
                    of the heights by 1
                if self.rank[x] == self.rank[y]:
28
                    self.rank[x] += 1
29
30
       def merge(self, x, y):
31
           x = self.find(x)
32
           y = self.find(y)
33
           if len(self.group[x]) < len(self.group[y]):</pre>
34
                x, y = y, x
35
           self.group[x].extend(self.group[y])
36
           self.group[y] = []
37
```

```
self.parent[y] = x
                                                                                           Resuelve las queries de intervalos y modificacion del array original
38
                                                                                    34
                                                                                           en O(log n)."""
                                                                                    35
39
       def check_same(self, x, y):
                                                                                           def __init__(self, n):
40
                                                                                    36
           return self.find(x) == self.find(y)
                                                                                                self.bit = [inf]*n #Binary Indexed Tree
41
                                                                                                self.n = n
42
                                                                                    38
       def get_size(self, x):
43
                                                                                    39
           return self.size[self.find(x)]
                                                                                           def initArray(self, array):
44
                                                                                    40
                                                                                               for i in range(len(array)):
                                                                                    41
                             2.2 FenwickTree
                                                                                                    self.update(i, array[i])
                                                                                    ^{42}
                                                                                    43
                                                                                           def getMin(self, r):
   class FenwickTreeSum:
                                                                                    44
                                                                                                ret = inf
       """ BIT de Sumas,
                                                                                    45
2
                                                                                                while(r>=0):
       Resuelve las queries de intervalos y modificacion del array original
                                                                                    46
3
       en O(log n)."""
                                                                                                    ret = min(ret, self.bit[r])
                                                                                    47
                                                                                                    r = (r&(r+1))-1
       def __init__(self, n):
                                                                                    48
5
           self.bit = [0]*n #Binary Indexed Tree
                                                                                    49
                                                                                                return ret
           self.n = n
                                                                                    50
7
                                                                                    51
8
       def initArray(self, array):
                                                                                    52
           for i in range(len(array)):
                                                                                           def update(self, idx, val):
                                                                                    53
10
                                                                                                while(idx<self.n):</pre>
               self.update(i, array[i])
                                                                                    54
11
                                                                                                    self.bit[idx] = min(self.bit[idx], val)
                                                                                    55
12
                                                                                                    idx \mid = (idx+1)
       def sum(self, r):
                                                                                    56
13
           ret = 0
                                                                                    57
14
                                                                                       """Revisar
           while(r>=0):
                                                                                    58
15
                                                                                       class FenwickTreeSum2D:
               ret += self.bit[r]
16
                                                                                           def __init__(self, n, m):
               r = (r&(r+1))-1
                                                                                    60
17
                                                                                               self.bit = [[0]*(m+1) for _ in range(n+1)] #Binary Indexed Tree
                                                                                    61
18
           return ret
19
                                                                                               self.n = n
20
                                                                                               self.m = m
       def rangeSum(self, 1, r):
                                                                                    63
21
                                                                                    64
           return self.sum(r)-self.sum(l-1)
22
                                                                                           def initArray(self,array):
                                                                                    65
23
                                                                                               aux = [[0]*(self.m+1) for _ in range(self.n+1)]
       def update(self, idx, delta): #Add delta to a[idx]
                                                                                    66
^{24}
                                                                                               for i in range(1,self.n+1):
           while(idx<self.n):</pre>
                                                                                    67
25
                                                                                                    for j in range(1,self.m+1):
               self.bit[idx] += delta
                                                                                    68
26
                                                                                                        aux[i][j] = array[self.n-j][i-1]
               idx = (idx+1)
                                                                                    69
27
                                                                                                #It's a matrix now
                                                                                    70
28
                                                                                                for j in range(1,self.m+1):
                                                                                    71
29
                                                                                                    for i in range(1,self.n+1):
                                                                                    72
30
                                                                                                        v1 = self.getSum(i,j)
                                                                                    73
   from math import inf
                                                                                                        v2 = self.getSum(i,j-1)
   class FenwickTreeMin:
                                                                                    74
32
                                                                                                        v3 = self.getSum(i-1,j-1)
       """ BIT de Min,
                                                                                    75
33
```

```
v4 = self.getSum(i-1,j)
                                                                                                      idx >>=1
76
                                                                                      15
                     self.update(i,j,aux[i][j]-(v1-v2-v4+v3))
                                                                                      16
77
                                                                                             def modifyInterval(self, 1, r, value):
                                                                                      17
78
        def getSum(self, i, j):
                                                                                                  """Modifica intervalo [1,r) poniendo value"""
79
                                                                                      18
            suma = 0
                                                                                                  l+=self.n; r+=self.n
                                                                                      19
80
            while(i>0):
                                                                                                  while(l<r):</pre>
81
                                                                                      20
                while(j>0):
                                                                                                      if(1&1):
82
                                                                                     21
                    suma += self.bit[i][j]
                                                                                                          l+=1; self.t[l]+= value
83
                                                                                      22
                    j = (j \& (j+1))-1
                                                                                                      if(r&1):
84
                                                                                      23
                i = (i \& (i+1))-1
                                                                                                          r-=1; self.t[r] += value
85
                                                                                                      1>>=1; r>>=1
            return suma
86
                                                                                     25
87
                                                                                     26
                                                                                             def push(self):
88
                                                                                     27
        def update( self, i, j, val):
                                                                                                  """Si necesitamos inspeccionar todos los elementos del array,
                                                                                      28
89
            while( i <= self.n ):</pre>
                                                                                                 es conveniente pushear la info a las hojas, reduce O(nlogn) a O(
                                                                                      29
90
                while(j <= self.m):</pre>
91
                                                                                                  0.00
                    self.bit[i][j] += val
92
                                                                                      30
                                                                                                 for i in range(1,self.n):
                    i = (i+1)
93
                                                                                     31
                i = (i+1)
                                                                                                      self.t[i<<1] += self.t[i]
                                                                                      32
94
                                                                                                      self.t[(i << 1)|1] += self.t[i]
                                                                                      33
95
        def answerQuery(self,i1,j1, i2, j2):
                                                                                                      self.t[i] = 0
                                                                                     34
96
            ans = self.getSum(i2+1, j2+1)-self.getSum(i2+1, j1)-self.getSum(
97
                                                                                      35
                                                                                             def query(self, l, r):
                i1, j2+1)+self.getSum(i1, j1)
                                                                                      36
                                                                                                  """Responde al intervalo [1,r)"""
98
                                                                                      37
                                                                                                  res = 0 #Se usa el neutro de la operacion
            return ans
                                                                                      38
99
    0.00
                                                                                                  l+=self.n ; r+=self.n
100
                                                                                      39
                                                                                      40
                                  Segment Tree
                                                                                                  while(l<r):</pre>
                                                                                      41
                                                                                                      if(1&1):
                                                                                      42
                                                                                                          res += self.t[1]
    class SegmentTree:
                                                                                      43
 1
                                                                                                          1+=1
        """Segment tree of sums"""
                                                                                      44
 2
                                                                                                      if(r&1):
                                                                                      45
 3
                                                                                                          r-=1
        def __init__(self, array):
                                                                                      46
 4
                                                                                                          res += self.t[r]
            self.n = len(array)
                                                                                      47
 5
                                                                                                      1>>=1: r>>=1
            self.t = [0]*self.n + array
                                                                                      48
 6
                                                                                      49
                                                                                                  return res
            for i in range(self.n-1, 0, -1):
                                                                                      50
 8
                self.t[i] = self.t[i << 1] + self.t[(i << 1) | 1]
                                                                                     51
 9
                                                                                             def queryElement(self, p):
                                                                                     52
10
                                                                                                  """Devuelve el valor de un elemento"""
                                                                                      53
        def modify(self, idx, val):
11
                                                                                                  res = 0; p+= self.n
            idx+=self.n; self.t[idx] = val
                                                                                     54
12
                                                                                                  while(p>0):
            while(idx>1):
                                                                                      55
13
                                                                                                      res+= self.t[p]
                self.t[idx>>1] = self.t[idx] + self.t[idx^1]
                                                                                     56
14
```

```
p>>=1
57
           return res
58
59
60
   a = SegmentTree([1,2,3,4])
   a.modifyInterval(0,3,10)
   print(a.queryElement(3))
   print(a.t)
65
   class SegmentTreeGeneric:
66
       """Generic Segment Tree. f es una funcion asociativa"""
67
68
       def __init__(self, array, f):
69
           self.n = len(array)
70
           self.t = [0]*self.n + array
71
           self.f = f #Me guardo la funcion aca para los otros metodos
72
73
           for i in range(self.n-1, 0, -1):
74
                self.t[i] = self.f(self.t[i << 1], self.t[(i << 1)|1])
75
76
       def modify(self, idx, val):
77
           idx+=self.n; self.t[idx] = val
78
           while(idx>1):
79
                self.t[idx>>1] = self.f(self.t[idx] + self.t[idx^1])
80
                idx >>=1
81
82
       def query(self, 1, r):
83
           res = 0 #Se usa el neutro de la operacion
84
           l+=self.n ; r+=self.n
85
86
           while(l<r):
87
                if(1&1):
88
                    res = self.t[l] if res==0 else self.f(res,self.t[l])
89
                    1+=1
90
                if(r&1):
91
92
                    res = self.t[r] if res==0 else self.f(self.t[r],res)
93
                1>>=1: r>>=1
94
95
           return res
96
```

## 2.4 Sparse Table

```
1 from math import log
2
   MAXN = 10**7 #Biggest possible array lenght
   K = 25 # Must satisfy K >= floor(log_2{MAXN})+1
   """Generic precomputation"""
   def precomputation(array, f):
       n = len(array)
       K = int(log(n,2))+1
       st = [[None for __ in range(K)] for _ in range(n)]
11
       for i in range(n):
12
           st[i][0] = f([array[i]])
13
       for j in range(1,K+1):
           for i in range(n-(1 << j)+1):
15
                st[i][j] = f([st[i][j-1], st[i+(1<<(j-1))][j-1]])
16
17
       return st
18
19
    """Range Sum Queries"""
   array = [1, 4, -1, 6, 9]
   n = len(array)
   K = int(log(n,2))+1
   st = precomputation(array, sum)
25
   def rangeSumQuery(L, R):
       sum = 0
27
       for j in range(K,-1,-1):
28
           if((1<<j) <= R-L+1):</pre>
29
                sum+= st[L][j]
30
                L += 1<<j
31
32
33
       return sum
34
35
    """Range Minimun Queries (RMQ)"""
   def precomputeLogs(n):
37
       logs = \{1:0\}
38
       for i in range(2,n+1):
39
           logs[i] = logs[i//2] + 1
40
41
       return logs
42
43
```

```
array = [1, 4, -1, 6, 9]
    n = len(array)
    K = int(log(n,2))+1
    st = precomputation(array, min)
    logs = precomputeLogs(n)

def rangeMinimumQuery( L, R):
    j = logs[R-L+1]
    return min(st[L][j], st[R-(1<<j)+1][j])</pre>
```

## 3 Graph

## 3.1 BFS

```
1 from collections import deque
   def bfs(ady, s):
     vis = set()
     parent = {}; dist = {}
     q = deque([])
     q.append(s); vis.add(s); parent[s]=-1; dist[s]=0
8
     while q:
9
       v = q.popleft()
10
       for u in adv[v]:
11
         if u not in vis:
12
           vis.add(u)
13
           q.append(u)
           dist[u] = dist[v]+1
           parent[u] = v
16
     return vis, parent, dist
17
18
   def SSSP(ady, src, dst):
19
     """Single-source shortest path"""
     vis, par , dist = bfs(ady,src)
21
     path = []
     if(dst not in vis): return path
23
     while(dst!=src):
24
       path.append(dst)
25
       dst = par[dst]
26
     path.append(src)
27
     return path[::-1]
                                 3.2 DFS
```

```
visited = set()
orden = []
def dfs(ady , v):
orden.append(v); visited.add(v)
for u in ady[v]:
if u not in visited:
dfs(ady,u)
```

## 3.3 Dijkstra

```
class Graph():
2
     def __init__(self, vertices):
3
       self.V = vertices
4
       self.graph = [[0 for column in range(vertices)]
5
             for row in range(vertices)]
6
7
     def printSolution(self, dist):
8
       print "Vertex_tDistance_from_Source"
9
       for node in range(self.V):
10
         print node, "t", dist[node]
11
12
     def minDistance(self, dist, sptSet):
13
14
       min = float('inf')
15
16
       for v in range(self.V):
17
         if dist[v] < min and sptSet[v] == False:</pre>
18
           min = dist[v]
19
           min index = v
20
21
       return min index
22
23
     def dijkstra(self, src):
24
^{25}
       dist = [sys.maxint] * self.V
26
       dist[src] = 0
27
       sptSet = [False] * self.V
28
29
       for cout in range(self.V):
30
         u = self.minDistance(dist, sptSet)
31
         sptSet[u] = True
32
33
         for v in range(self.V):
34
           if self.graph[u][v] > 0 and sptSet[v] == False and \
35
           dist[v] > dist[u] + self.graph[u][v]:
36
                dist[v] = dist[u] + self.graph[u][v]
37
38
       self.printSolution(dist)
39
```

## 3.4 Floyd-Warshall

```
def floydWarshall(adyMatrix):
     "APSP_problem,_0(V^3)"
     v = len(adyMatrix)
     for k in range(v):
       for i in range(v):
         for j in range(v):
6
           adyMatrix[i][j] = min(adyMatrix[i][j],adyMatrix[i][k]+adyMatrix[
               k][j])
8
   def transitiveClosure(d):
     """d[i][j] tiene 1 si hay un camino enre i y j,
      O en caso contrario, O(V^3)"""
12
     v = len(d)
13
     for k in range(v):
       for i in range(v):
         for j in range(v):
16
           d[i][j] = (d[i][k] & d[k][j])
18
   def minimax(d):
     """Encuentra el minimo entre los maximos edges de cada path"""
     v = len(d)
22
     for k in range(v):
23
       for i in range(v):
24
         for j in range(v):
25
           d[i][j] = min(d[i][k], max(d[i][k],d[k][j]))
26
27
   def maximin(d):
28
     v = len(d)
    for k in range(v):
30
       for i in range(v):
31
         for j in range(v):
32
           d[i][j] = max(d[i][j], min(d[i][k],d[k][j]))
33
             3.5 Max Flow-Min Cut (Ford Fulkerson)
1 from collections import deque
2 from math import inf
   class Graph:
       def __init__(self, cap):
           self.n = len(cap)
5
           self.cap = cap
6
```

```
self.org_cap = [i[:] for i in cap]
7
       def bfs(self,s,t,parent):
8
           visited = [False]*(self.n)
9
           queue = deque([])
10
           queue.append(s); visited[s]=True
11
           while queue:
12
               u = queue.popleft()
13
               for ind,val in enumerate(self.cap[u]):
14
                    if(not visited[ind] and val):
15
                        queue.append(ind)
16
                        visited[ind] =True
17
                        parent[ind] = u
18
           return visited[t]
19
20
       def FordFulkerson(self, source, sink):
21
           parent = [-1]*(self.n)
22
           max_flow = 0
23
           while self.bfs(source,sink,parent):
24
               path_flow = inf
25
               s = sink
26
               while(s!=source):
27
                   path_flow = min(path_flow,self.cap[parent[s]][s])
28
                    s = parent[s]
29
               max_flow += path_flow
30
               v = sink
31
               while(v!= source):
32
                    u = parent[v]
33
                   self.cap[u][v] -= path_flow
34
                   self.cap[v][u] += path_flow
35
                   v = parent[v]
36
           return max flow
37
38
39
       def minCut(self, source, sink):
40
           def dfs(s,visited):
41
               visited[s] = True
42
               for u in range(self.n):
43
                    if (not visited[u] and self.cap[s][u]>0):
44
                        dfs(u, visited)
45
           g.FordFulkerson(source,sink)
46
           print(g.cap)
47
           vis = [False]*self.n
48
           dfs(source, vis)
49
```

## 4 Math

#### 4.1 Identities

```
C_n = \frac{2(2n-1)}{n+1}C_{n-1}
C_n = \frac{1}{n+1}\binom{2n}{n}
C_n \sim \frac{4^n}{n^{3/2}\sqrt{\pi}}
\sigma(n) = O(\log(\log(n))) \text{ (number of divisors of } n)
F_{2n+1} = F_n^2 + F_{n+1}^2
F_{2n} = F_{n+1}^2 - F_{n-1}^2
\sum_{i=1}^n F_i = F_{n+2} - 1
F_{n+i}F_{n+j} - F_nF_{n+i+j} = (-1)^n F_i F_j
\sum_{i=1}^n i^k = \frac{1}{k+1}(\sum_{j=1}^{k+1} \binom{k+1}{j} n^j - \sum_{j=0}^{k-1} \binom{k+1}{j} i^j)
S_k(n) = \frac{1}{k+1}((n+1)^{k+1} - 1 - (\sum_{j=2}^{k+1} \binom{k+1}{j}) S_{k+1-j}(n)))
(Möbius Inv. Formula) Let g(n) = \sum_{d|n} f(d), then f(n) = \sum_{d|n} g(d) \mu\left(\frac{n}{d}\right).
```

#### 4.2 GCD

```
gcd = lambda a, b : a if(b==0) else gcd(b,a%b)

def it_gcd(a, b):
    while(b):
    a%=b
    a, b = b, a #Swap para tener el mas chico en b
return a
```

## 4.3 Euler Totient (Phi)

```
def phi(n):
1
     """O(sqrt(n)) approach using factorization"""
     result = n
3
     i=2
4
     while(i*i<=n):</pre>
       if(n%i==0):
6
          while(n\%i == 0):
7
            n//=i
8
         result -= result//i
9
       i+=1
10
     if(n>1):
11
       result-= result//n
12
13
     return result
14
```

#### 4.4 Extended Euclides

```
def gcd(a, b):
       """Devuelve el gcd entre a y b, y coefx y coefy tales
       que a*coefx+b*coefy = gcd"""
       if(a==0):
           return b, 0, 1
5
       d, x1, y1 = gcd(b\%a, a)
       x = y1-(b//a)*x1
       y = x1
       return d, x, y
11
   def modinv(a, m):
       g, x, y = gcd(a,m)
13
       if(g!=1):
14
           return None
15
       x = (x\%m + m)\%m
16
       return x
17
                              4.5 Modexp
  def modexp( x, y, p ):
     """Exponenciacion logaritmica iterativa,
     x^y (mod p), el orden el O(log y)"""
4
     res = 1
5
     while(y>0):
      if(y & 1):
        res*= x
        res%=p
       y >>= 1
       x = x
12
     return res%p
13
14
15
   """Inverso si m es primo"""
modinv = lambda a, m : modexp(a, m-2, m)
                             4.6 allModInv
```

1 """Find all invmods in range [1,m-1] in O(m)"""

```
def allModInvs(m):
    inv = [1]*(m) #Remember that inv[i] has the inverse of i
    inv[0] = None
    for i in range(2,m):
        inv[i] = -(m//i)*inv[m%i] %m

return inv
```

## 4.7 Iter multiplication

```
def logmul(a, b):
       """No creo que sea necesario en python, pero version recursiva
2
       de la multiplicacion que sirve en C++"""
       if(a == 0):
           return 0
       return 2*logmul((a-1)//2,b)+b if (a\%2) else 2*logmul(a//2,b)
   def logmulmod(a, b, p):
       """Multiplicacion recursiva mod p"""
10
       if(a == 0):
11
           return 0
12
13
       res = 2*logmulmod((a-1)//2,b, p)+b if (a\%2) else 2*logmulmod(a//2,b,
14
           p)
       return res%p
15
```

# 4.8 Test de primalidad y Descomposicion en Primos 4.8.1 Is Prime

```
def is_prime(n):
       """Naive O(sqrt(n)) approach"""
2
       d = 2
3
       while(d*d<=x):</pre>
4
           if(x%d == 0):
5
               return False
6
           d+=1
       return True
  from random import randint
11
  |RAND_MAX| = 10**9
def modexp(x, y, p):
```

```
res = 1
14
     while(y>0):
15
       if(y & 1):
16
         res*= x
17
         res%=p
18
       y >>= 1
       x*= x
21
     return res%p
22
23
   def probablyPrimeFermat(n, iter=5):
24
       if (n < 4):
25
           return n == 2 or n == 3
26
27
       for i in range(iter):
28
           a = 2 + randint(1, RAND_MAX)\%(n - 3);
29
           if (modexp(a, n - 1, n)!=1):
30
                return False
31
32
       return True
   for i in range(100):
       print(i,probablyPrimeFermat(i,5))
36
```

#### 4.8.2 Miller Rabin Test

```
1 | from random import randint
   RAND_MAX = 10**9
   def modexp( x, y, p ):
     res = 1
     while(y>0):
       if(v & 1):
6
         res*= x
         res%=p
       v >>= 1
       x*= x
11
     return res%p
12
13
   def check_composite( n, a, d, s):
       x = modexp(a, d, n)
15
       if (x == 1 \text{ or } x == n - 1):
16
            return False
17
```

```
for r in range(1,s):
                                                                                   61 for i in range(100000):
18
           x = x * x % n;
                                                                                           if(MillerRabin(i)):
                                                                                   62
19
           if (x == n - 1):
                                                                                               cnt+=1
20
               return False
                                                                                   64 print(cnt)
21
22
                                                                                                                4.8.3 Prime Factors
       return True
23
^{24}
   def MillerRabinProb(n, iter = 5):
                                                                                    # Program to fiind prime factors and their powers
25
       """Returns true if n is probably prime, else returns false."""
                                                                                    # using Sieve Of Eratosthenes
26
       if (n < 4):
27
           return n == 2 or n == 3
                                                                                       def sieveOfEratosthenes(N, s):
28
                                                                                           """Sieve with smaller prime factor of s[i]"""
29
       s = 0:
30
       d = n - 1:
                                                                                           prime = [False] * (N+1)
31
                                                                                    7
       while ((d \& 1) == 0):
32
                                                                                    8
           d >>= 1;
33
                                                                                           for i in range(2, N+1, 2):
                                                                                    9
           s+=1
34
                                                                                               s[i] = 2
                                                                                   10
35
                                                                                   11
       for i in range(iter):
                                                                                           for i in range(3, N+1, 2):
36
                                                                                   12
           a = 2 + randint(1,RAND_MAX) \% (n - 3);
                                                                                               if (prime[i] == False):
37
                                                                                   13
           if(check_composite(n, a, d, s)):
                                                                                                   s[i] = i
38
               return False
39
                                                                                   15
       return True
                                                                                                   for j in range(i, N//i + 1, 2):
40
                                                                                   16
                                                                                                       if (prime[i*j] == False):
41
                                                                                   17
                                                                                                           prime[i*j] = True
42
                                                                                   18
    """Deterministic Version"""
                                                                                                            s[i * j] = i
                                                                                   19
   def MillerRabin(n):
44
                                                                                   20
       if(n<2):
45
                                                                                   21
           return False
                                                                                      def generatePrimeFactors(N):
46
                                                                                   22
47
                                                                                   23
       r = 0
48
                                                                                           #s[i]: smallest prime factor
                                                                                   24
       d = n - 1
                                                                                           s = [0] * (N+1)
49
                                                                                   25
       while ((d \& 1) == 0):
                                                                                           sieveOfEratosthenes(N, s)
50
                                                                                   26
           d >>= 1
51
                                                                                   27
           r+=1
                                                                                           factors = [] #Contains tuples (p_i, alpha_i)
52
                                                                                   28
53
                                                                                   29
       for a in {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37}:
                                                                                           curr = s[N]
54
                                                                                   30
           if (n == a):
                                                                                           # Power of current prime factor
55
                                                                                   31
               return True
                                                                                           cnt = 1
56
                                                                                   32
           if(check_composite(n, a, d, r)):
57
                                                                                   33
               return False
                                                                                           while (N > 1):
58
                                                                                   34
       return True
                                                                                               N //= s[N]
59
                                                                                   35
  | cnt = 0
                                                                                   36
```

```
if (curr == s[N]):
                                                                                      def trial_division3(n):
37
                cnt += 1
                                                                                             factorization = []
                                                                                     34
38
                                                                                             for d in \{2,3,5\}:
                continue
39
                                                                                     35
                                                                                                 while(n%d==0):
40
                                                                                     36
           factors.append((curr,cnt))
                                                                                                      factorization.append(d)
41
                                                                                     37
           curr = s[N]
                                                                                                      n //= d
42
                                                                                      38
           cnt = 1
43
                                                                                     39
       return factors
                                                                                             increments = [4, 2, 4, 2, 4, 6, 2, 6]
44
                                                                                      40
                                                                                             i = 0
                                                                                     41
                              4.8.4 Integer Fact
                                                                                             d = 7
                                                                                             while(d*d<=n):</pre>
                                                                                     43
                                                                                                 while(n\%d == 0):
   """Naive O(sqrt(n)) approach"""
                                                                                      44
   def trial_division1(n):
                                                                                                      factorization.append(d)
                                                                                      45
2
                                                                                                      n//=d
       factorization = []
3
                                                                                                 i %= 8
       d = 2
                                                                                     47
4
                                                                                                 d+=increments[i]
       while(d*d<=n):</pre>
5
           while(n\%d == 0):
                                                                                     49
6
                                                                                             if(n>1):
               factorization.append(d)
                                                                                     50
                                                                                                 factorization.append(n)
                n//=d
                                                                                     51
8
                                                                                             return factorization
           d+=1
                                                                                     52
9
                                                                                     53
10
       if(n>1):
                                                                                     54
11
                                                                                          """Precomputed primes"""
           factorization.append(n)
                                                                                      55
12
       return factorization
                                                                                      56
13
                                                                                     57
14
    """Don't try even numbers if it's odd. (Wheel factorization)"""
                                                                                      58
15
                                                                                         def trial_division4(n):
   def trial_division2(n):
                                                                                      59
16
                                                                                             """Fast way to find primes"""
       factorization = []
                                                                                      60
17
                                                                                             MAX_PRIME = 10**6
       while(n\%2 == 0):
                                                                                     61
18
                                                                                             def listPrimesFast(max n):
                                                                                     62
           factorization.append(2)
19
                                                                                                 """sundaram3"""
           n >>= 1
                                                                                     63
20
                                                                                                 numbers = [i for i in range(3, max_n+1, 2)]
                                                                                     64
21
                                                                                                 half = (max n)//2
       d = 3
                                                                                     65
^{22}
                                                                                                 initial = 4
       while(d*d<=n):</pre>
                                                                                     66
23
           while (n\%d==0):
                                                                                     67
24
                                                                                                 for step in range(3, max_n+1, 2):
                                                                                     68
                factorization.append(d)
^{25}
                                                                                                      for i in range(initial, half, step):
                n //= d
                                                                                     69
26
                                                                                                          numbers[i-1] = 0
           d+=2
                                                                                     70
27
                                                                                                      initial += 2*(step+1)
       if(n>1):
                                                                                     71
28
           factorization.append(n)
                                                                                     72
29
                                                                                                 if initial > half:
       return factorization
                                                                                     73
30
                                                                                                      return [2] + filter(None, numbers)
                                                                                     74
31
   """Same Wheel idea, but with factors 2,3,5 at the same time."""
                                                                                     75
```

```
primes = listPrimesFast(MAX_PRIME)
                                                                                                   x = x
76
                                                                                      119
        factorization = []
77
                                                                                      120
        for d in primes:
                                                                                                 return res%p
78
                                                                                      121
            if(d*d>n):
79
                                                                                      ^{122}
                 break
                                                                                               B = 10
                                                                                      123
80
            while(n\%d == 0):
                                                                                               g = 1
81
                                                                                      124
                 factorization.append(d)
                                                                                               primes = listPrimesFast(MAX_PRIME)
82
                                                                                      125
                                                                                               while(B <= 10**7 and g<n):
83
                                                                                      126
        if(n>1):
                                                                                                   a = 2 + randint(1,MAX_RAND) \% (n-3)
84
                                                                                      127
            factorization.append(n)
                                                                                                   g = gcd(a,n)
85
                                                                                                   if(g>1):
86
                                                                                      129
        return factorization
                                                                                                       return g
87
                                                                                      130
88
                                                                                      131
                                                                                                   #Computo a^M
                                                                                      132
89
    """Pollard's p-1 method"""
                                                                                                   for p in primes:
                                                                                      133
    from random import randint
                                                                                                       if(p>=B):
   from math import gcd
                                                                                                            continue
                                                                                       135
    MAX_RAND = 10**9
                                                                                                       p_power = 1
                                                                                       136
                                                                                                       while(p_power * p <= B):</pre>
    def pollard_p_minus_1(n):
                                                                                      137
94
        """Probabilistic method, O(BlogB log^2 n), encuentra un primo
                                                                                                            p_power *= p
                                                                                      138
95
        que divide a n"""
                                                                                                       a = modexp(a, p_power, n)
                                                                                      139
96
        MAX_PRIME = 10**6
97
                                                                                      140
        def listPrimesFast(max_n):
                                                                                                       g = gcd(a-1, n)
                                                                                      141
98
            """sundaram3"""
                                                                                                       if (g>1 \text{ and } g< n):
                                                                                      142
99
            numbers = [i for i in range(3, max_n+1, 2)]
                                                                                                            return g
                                                                                      143
100
            half = (max_n)//2
                                                                                                   B*=2
                                                                                      144
101
            initial = 4
                                                                                      145
102
                                                                                      146
                                                                                              return 1
103
            for step in range(3, max_n+1, 2):
                                                                                      147
104
                 for i in range(initial, half, step):
105
                                                                                      148
                     numbers[i-1] = 0
                                                                                           """Pollard Rho algorithm to find a factor of n"""
106
                                                                                      149
                 initial += 2*(step+1)
                                                                                          from math import gcd
107
                                                                                          def floyd(f, x0):
108
            if initial > half:
                                                                                              tortoise = x0
109
                 return [2] + list(filter(None, numbers))
                                                                                              hare = f(x0)
                                                                                      153
110
                                                                                               while(tortoise != hare):
                                                                                      154
111
                                                                                                   tortoise = f(tortoise)
        def modexp( x, y, p ):
                                                                                      155
112
          res = 1
                                                                                                   hare = f(f(hare))
113
                                                                                      156
          while(y>0):
                                                                                      157
114
            if(v & 1):
                                                                                              return true
                                                                                      158
115
              res*= x
116
                                                                                      mult = lambda a, b, mod: a*b % mod
              res%=p
117
                                                                                      f = lambda x, c, mod: (mult(x,x,mod)+c) mod
            y >>= 1
118
```

37

38

b //= g

```
162
    def rho(n, x0=2, c=1):
163
        x, y, g = x0, x0, 1
164
        while(g==1):
165
            x = f(x, c, n)
166
            y = f(y, c, n)
167
            y = f(y, c, n)
168
             g = gcd(abs(x-y), n)
169
170
        return g
171
172
173
     """Brent, direct implementation"""
174
    from math import gcd
175
    mult = lambda a, b, mod: a*b % mod
176
    f = lambda x, c, mod: (mult(x,x,mod)+c) mod
177
178
    def brent(n, x0 = 2, c=1):
179
        x, g, q = x0, 1, 1
180
        m = 128
181
        1 = 1
182
        while(g==1):
183
            y = x
184
             for i in range(1,1):
185
                 x = f(x, c, n)
186
             k = 0
187
188
             while(k<l and g==1):</pre>
189
                 xs = x
190
                 i = 0
191
                 while(i<m and i<l-k):
192
                      x = f(x, c, n)
193
                      q = mult(q, abs(y-x), n)
194
                      i+=1
195
                 g = gcd(q, n)
196
                 k+=m
197
             1*=2
198
199
        if(g==n):
200
             while True:
201
                 xs = f(xs, c, n)
202
                 g = gcd(abs(xs-y), n)
203
                 if (g!=1 \text{ and } g!=n):
204
```

```
break
205
206
       return g
                                  Diofanticas
                              4.9
 def gcd(a, b):
       """Devuelve el gcd entre a y b, y coefx y coefy tales
       que a*coefx+b*coefy = gcd"""
       if(a==0):
           return b, 0, 1
       g, x1, y1 = gcd(b%a, a)
       x = y1 - (b//a) * x1
7
       y = x1
 8
       return g, x, y
10
   def find_any_solution(a, b, c):
11
        """Returns g = gcd(a,b) and a pair of coef x0, y0 such that
12
       a*x0+b*y0 = g'''''
13
       g, x0, y0 = gcd(abs(a), abs(b))
       if (c % g):
           return False
17
       x0 *= c // g;
18
       y0 *= c // g;
19
       if (a < 0): x0 = -x0;
       if (b < 0): y0 = -y0;
21
       return g, x0, y0
23
24
   def shift_solution(x, y, a, b, cnt):
       """Dada una solucion a la ecuacion diofantica, encuentra otra"""
       x += cnt * b;
27
       y -= cnt * a;
28
       return x, y
29
30
31
   def find_all_solutions( a, b, c, minx, maxx, miny, maxy):
       sol = find_any_solution(a, b, c)
33
       if (not sol):
34
           return 0
35
       g, x, y = sol
36
       a //= g
```

```
39
       sign_a = 1 if(a > 0) else -1
40
       sign_b = 1 if(b > 0) else -1
41
42
       x, y = shift_solution(x, y, a, b, (minx - x) // b)
43
       if (x < minx):
44
           x, y = shift_solution(x, y, a, b, sign_b)
45
       if (x > maxx):
46
           return 0
47
       1x1 = x
48
49
       x, y = shift_solution(x, y, a, b, (maxx - x) // b);
50
       if (x > maxx):
51
           x, y = shift_solution(x, y, a, b, -sign_b)
52
       rx1 = x
53
54
       x, y = shift_solution(x, y, a, b, -(miny - y) // a)
55
       if (y < miny):</pre>
56
           x, y = shift_solution(x, y, a, b, -sign_a)
57
       if (y > maxy):
58
           return 0
59
       1x2 = x
60
61
       x, y = shift_solution(x, y, a, b, -(maxy - y) // a)
62
       if (y > maxy):
63
           shift_solution(x, y, a, b, sign_a)
64
       rx2 = x
65
66
       if (1x2 > rx2):
67
           1x2, rx2 = rx2, 1x2
68
       lx = max(lx1, lx2);
69
       rx = min(rx1, rx2);
70
71
       if (lx > rx):
72
           return 0
73
74
       # Para enumerarlas, basta iterar desde x = lx + k*b//g, el numero
75
       # necesario de soluciones
76
77
       return (rx - lx) // abs(b) + 1;
78
```

#### 4.10 Cribas

#### 4.10.1 Criba Primos

```
"""Criba sin optimizar, O(n* log log n)"""
  n = 10**6
   is_prime = [True] * (n+1)
   is_prime[0] = False
   is_prime[1] = False
   for i in range(2,n+1):
     if(is_prime[i] and i*i<=n):</pre>
       for j in range(i*i,n+1,i):
11
         is_prime[j] = False
12
13
14
   """Sieving till root"""
15
16
   n = 10**6
   is_prime = [True]*(n+1)
   is_prime[0] = False
   is_prime[1] = False
22
   for i in range(2,n+1):
    if(is_prime[i]):
24
       for j in range(i*i,n+1,i):
         is_prime[j] = False
26
                            4.10.2 Block Sieving
   """Cuento los primos menores a n usando block_sieving"""
2
   def count_primes(n):
     S = 10000
     primes = []
     nsqrt = int(n**0.5)
     is_prime = [True]*(nsqrt+1)
7
8
     for i in range(2, nsqrt+1):
9
       if(is_prime[i]):
10
```

primes.append(i)

11

```
for j in range(i*i,nsqrt+1,i):
12
            is_prime[j] = False
13
14
     result = 0
15
     block = [True] *S
16
17
     k = 0
18
     while(k*S \le n):
19
       block = [True] *S
20
       start = k*S
21
22
       for p in primes:
23
          start_idx = (start+p-1)//p
24
          j = max(start_idx, p )* p - start
25
          while(j<S):</pre>
26
            block[j] = False
27
            j+=p
28
29
       if(k == 0):
30
            block[0] = False
31
            block[1] = False
32
       i = 0
33
       while(i<S and start+i <= n):</pre>
34
         if(block[i]):
35
           result+=1
36
         i+=1
37
       k+=1
38
39
     return result
40
                              4.10.3 Linear Sieve
```

```
j = 0
12
       while(j<len(pr) and pr[j]<=lp[i] and i*pr[j]<=N):</pre>
13
           lp[i*pr[j]] = pr[j]
14
           j+=1
15
   end = timeit.default_timer()
   print(end-start)
   print(lp[:20])
20 | print(pr[:20])
                              4.11 Divisores
                           4.11.1 Count Divisors
   def countDivisors(n):
       """Naive implementation to count divisors of n, in O(sqrt(n))"""
3
       for i in range(1, int(n**0.5)+1):
4
           if (n % i == 0):
5
                cnt += 1 if(i*i == n) else 2
7
       return cnt
8
10
11
   """Improved method in O(n^{(1/3)})"""
   def SieveOfEratosthenes(n, prime,primesquare, a):
       """Sieve of primes and squares of primes."""
14
       for i in range(2,n+1):
15
           prime[i] = True
16
17
       for i in range((n * n + 1)+1):
18
           primesquare[i] = False
19
20
       prime[1] = False
21
22
       p = 2
23
       while(p * p \le n):
24
           if (prime[p] == True):
25
               i = p * 2
26
                while(i <= n):</pre>
27
                    prime[i] = False
28
                    i += p
29
           p+=1
30
```

```
31
                                                                                  74
       j = 0
                                                                                  75
                                                                                          return ans
32
       for p in range(2,n+1):
33
                                                                                                              4.11.2 Suma Divisores
           if (prime[p] == True):
34
               a[j] = p
35
                                                                                   1 # Sum of all divisors of n.
36
                                                                                   def sumofFactors(n):
               primesquare[p * p] = True
37
                                                                                          res = 1
               j+=1
38
                                                                                         for i in range(2, int(n**0.5 + 1)):
39
                                                                                              curr_sum = 1
   def countDivisorsFast(n):
                                                                                              curr_term = 1
       """Count divisors in O(n^{(1/3)})"""
41
                                                                                   7
       if (n == 1):
42
                                                                                              while n \% i == 0:
           return 1
43
                                                                                                  n //= i
44
                                                                                                  curr_term *= i
       prime = [False]*(n + 2)
45
                                                                                                  curr_sum += curr_term;
                                                                                  11
       primesquare = [False]*(n*n+2)
46
47
                                                                                              res *= curr_sum
                                                                                  13
       a = [0]*n
48
                                                                                  14
49
                                                                                          if n > 2:
                                                                                  15
       SieveOfEratosthenes(n, prime, primesquare, a)
50
                                                                                              res *= (1 + n)
                                                                                  16
51
                                                                                  17
       ans = 1
52
                                                                                          return res
                                                                                  18
53
                                                                                                                 4.12 Factorial
       i=0
54
       while(1):
55
                                                                                                              4.12.1 Factorial mod
           if(a[i]**3 > n):
56
               break
57
                                                                                   def factmod(n, p):
58
                                                                                         """O(p log n ) aproach to calculate n! (mod p)"""
           cnt = 1
59
                                                                                          if(n>p):
                                                                                   3
           while (n \% a[i] == 0):
60
                                                                                              return 0
                                                                                   4
               n //= a[i]
61
                                                                                          res = 1
                                                                                   5
               cnt += 1
62
                                                                                          while(n > 1):
           ans *= cnt
63
                                                                                              res = (res* (p-1 if((n//p)%2) else 1)) % p;
           i+=1
64
                                                                                              for i in range(2, n%p+1):
65
                                                                                                  res = (res * i) % p
       if(prime[n] == True):
66
                                                                                              n //= p
                                                                                  10
           ans *= 2
67
                                                                                  11
68
                                                                                         return res % p;
       elif(primesquare[n] == True):
69
           ans *= 3
                                                                                                            4.12.2 Factorial Divisors
70
71
       elif(n != 1):
                                                                                   # Count of divisors of n!
72
           ans *= 4
73
                                                                                   2
```

```
3 | allPrimes = []
   def sieve(n):
       prime = [True] * (n + 1)
6
       p = 2
       while(p * p \le n):
8
           if (prime[p] == True):
9
                i = p * 2
10
                while(i <= n):</pre>
11
                    prime[i] = False
12
                    i += p
13
           p += 1
14
15
       for p in range(2, n + 1):
16
           if (prime[p]):
17
                allPrimes.append(p)
18
19
   def factorialDivisors(n):
21
       sieve(n)
22
       result = 1
23
24
       for i in range(len(allPrimes)):
25
           p = allPrimes[i]
26
           exp = 0
27
            while (p \le n):
28
                exp += n // p
29
                p *= allPrimes[i]
30
31
           result *= (exp + 1)
32
33
       return result
34
                                  4.13 FFT
  from cmath import exp
```

```
from cmath import exp
from math import pi

# A simple class to simulate n-th root of unity
class NthRootOfUnity:
    def __init__(self, n, k = 1):
        self.k = k
```

self.n = n

8

```
9
       def __pow__(self, other):
10
           if type(other) is int:
11
                n = NthRootOfUnity(self.n, self.k * other)
12
                return n
13
14
       def __eq__(self, other):
15
           if other == 1:
16
                return abs(self.n) == abs(self.k)
17
18
       def __mul__(self, other):
19
           return exp(2*1j*pi*self.k/self.n)*other
20
21
       def __repr__(self):
22
           return str(self.n) + "-th, root, of, unity, to, the, " + str(self.k)
23
24
       @property
25
       def th(self):
           return abs(self.n // self.k)
27
29
   """ The Fast Fourier Transform Algorithm
31
    Input: A, An array of integers of size n representing a polynomial
           w , a n-root of unity
33
    Output: [A(w), A(w^2), \ldots, A(w^{(n-1))}]
    Complexity: O(n logn)"""
35
   def FFT(A, omega):
       if omega == 1:
37
           return [sum(A)]
       o2 = omega**2
       C1 = FFT(A[0::2], o2)
       C2 = FFT(A[1::2], o2)
       C3 = [None] *omega.th
       for i in range(omega.th//2):
           C3[i] = C1[i] + omega**i * C2[i]
           C3[i+omega.th//2] = C1[i] - omega**i * C2[i]
45
       return C3
46
   """ The Fast Polynomial Multiplication Algorithm
    Input: A,B, two arrays of integers representing polynomials
    (coef in increasing deg) their length is in O(n)
```

32

```
Output: Coefficient representation of AB
52
    Complexity: O(n logn)"""
53
   def FPM(A,B):
54
       n = 1 << (len(A) + len(B) - 2).bit_length()
55
       o = NthRootOfUnity(n)
56
       AT = FFT(A, o)
57
       BT = FFT(B, o)
58
       C = [AT[i]*BT[i] for i in range(n)]
59
       D = [round((a/n).real) \text{ for a in } FFT(C, o ** -1)]
60
       while len(D) > 0 and D[-1] == 0:
61
           del D[-1]
62
       return D
63
```

## 4.14 Lagrange Interpolation

```
def interpolacion(muestra, x):
     """Recibe una muestra de n puntos (tuplas (xi,yi))
     y evalua el polinomio de Lagrange de
3
     en el punto x desconocido"""
4
     ans = 0
5
     n = len(muestra)
6
     for i in range(n):
       term = muestra[i][1]
8
       for j in range(n):
9
         if(j!=i):
10
           term = term*(x-muestra[j][0])/(muestra[i][0]-muestra[j][0])
11
       ans+=term
12
     return ans
13
```

## 4.15 Discrete Log

```
def discreteLog(a, b, m):
       n = int(m**0.5) + 1
2
       an = 1;
3
       for i in range(n):
4
           an = (an * a) \% m
5
6
       vals = {}
       cur = an
8
       for p in range(1,n+1):
9
           if not cur in vals:
10
               vals[cur] = p
11
           cur = (cur * an) % m
12
13
```

```
cur = b
for q in range(n+1):
if cur in vals:
ans = vals[cur] * n - q
return ans
cur = (cur * a) % m

return -1
```

#### 4.16 Discrete Root

```
1 from math import gcd
   def modexp( x, y, p ):
     """Exponenciacion logaritmica iterativa,
     x^y (mod p), el orden el O(log y)"""
5
6
     res = 1
7
     while(y>0):
       if(y & 1):
         res*= x
         res%=p
11
       y >>= 1
       x = x
13
14
     return res%p
15
16
17
   # Finds the primitive root modulo p
   def generator(p):
       fact = []
20
       phi = p-1
21
       n = phi
22
       i = 2
23
       while(i*i<=n):</pre>
24
           if(n \% i == 0):
25
                fact.append(i);
26
                while (n \% i == 0):
27
                    n //= i
28
           i+=1
29
30
       if(n > 1): fact.push_back(n)
31
```

```
for res in range(2,p+1):
33
           ok = True;
34
           for factor in fact:
35
               if(modexp(res, phi // factor, p) == 1):
36
                   ok = False
37
                   break
38
           if(ok): return res
39
       return -1;
40
                                Primitive Root
```

```
from math import sqrt
   def isPrime(n):
       if (n \le 1):
            return False
5
       if (n \le 3):
6
            return True
7
8
       if (n \% 2 == 0 \text{ or } n \% 3 == 0):
9
            return False
10
       i = 5
11
       while(i * i \le n):
12
            if (n \% i == 0 \text{ or } n \% (i + 2) == 0):
13
                 return False
14
            i = i + 6
15
16
       return True
17
18
   def modexp( x, y, p ):
19
     res = 1
20
      while(y>0):
21
       if(y & 1):
^{22}
         res*= x
23
         res%=p
24
       y >>= 1
25
       x = x
26
27
     return res%p
28
29
30
   """O(log^6 p)"""
  def findPrimefactors(s, n):
```

```
while (n \% 2 == 0):
33
            s.add(2)
34
           n //= 2
35
36
       for i in range(3, int(sqrt(n)), 2):
37
           while (n \% i == 0):
38
                s.add(i)
39
                n //= i
40
41
       if (n > 2):
           s.add(n)
43
44
   def findPrimitive(n):
       s = set()
47
       if (isPrime(n) == False):
           return -1
49
50
       phi = n-1
51
       findPrimefactors(s, phi)
53
       for r in range(2, phi + 1):
54
           flag = False
55
            for it in s:
56
                if (modexp(r, phi // it, n) == 1):
57
                    flag = True
58
                    break
59
            if (flag == False):
60
                return r
61
       return -1
62
```

#### 4.18 Fibonacci

Notebook Python 4 MATH - 4.19 Gray Code Page 22 of 27

```
11
   def matrix_exp( A, n ):
12
     """Exponenciacion logaritmica iterativa de matrices,
13
     A^n, el orden es O(d^3*log n), con d la dimension de la
     matriz"""
16
     res = identity(len(A))
17
     while(n>0):
18
       if(n & 1):
19
         res = matrix_multiplication(res,A)
20
21
       n >>= 1
22
       A = matrix_multiplication(A, A)
23
^{24}
     return res
25
26
   def fibo_log(n):
27
       """Returns f_n, using matrix log exponenciation"""
28
       f = \lceil \lceil 0 \rceil, \lceil 1 \rceil \rceil
29
       transition = [[0,1],[1,1]]
30
       result = matrix_multiplication(matrix_exp(transition,n),f)
31
       return result[0][0]
32
33
    """Could lead to a WA, but O(1) solution (check if **n does not lead to
34
       O(n)
35
   def fibo_approx(n):
36
       phi, phi_conj = (1+5**0.5)/2, (1-5**0.5)/2
37
38
       return round((phi**n-phi_conj**n)/(5**0.5))
39
40
41
    """Fast doubling Method"""
42
   def fibo_fast_doubling(n):
       if (n == 0):
44
            return (0, 1)
45
46
       p = fibo_fast_doubling(n >> 1)
47
       c = p[0]*(2*p[1]-p[0])
48
       d = p[0]**2 + p[1]**2
49
       return (d, c + d) if (n & 1) else (c, d)
50
```

## 4.19 Gray Code

```
def g(n):
    return n^(n>>1)

def rev_g(g):
    n = 0
    while(g):
    n^=g
    g>>=1
    return n
```

## 4.20 Matrix

```
matrix_sum = lambda X,Y: [list(map(sum, zip(*t))) for t in zip(X, Y)]
matrix_sum = lambda X,Y: [list(map(sum, zip(*t))) for t in zip(X, Y)]
```

12

## 5 Geo

#### 5.1 Convex Hull

```
1 from functools import reduce
  def convex_hull_graham(points):
       TURN_LEFT, TURN_RIGHT, COLLINEAR = (1, -1, 0)
3
       def cmp(a, b):
4
           return (a > b) - (a < b)
5
6
       def turn(p, q, r):
7
           return cmp((q[0] - p[0])*(r[1] - p[1]) - (r[0] - p[0])*(q[1] - p
8
9
       def _keep_left(hull, r):
10
           while len(hull) > 1 and turn(hull[-2], hull[-1], r) not in {
11
               TURN_LEFT }:
             #Agregar a {TURN_LEFT} el elemento COLLINEAR si se quieren
12
                 alineados en
             #En la frontera
13
               hull.pop()
14
           if not len(hull) or hull[-1] != r:
15
               hull.append(r)
16
           return hull
17
18
       points = sorted(points)
19
       1 = reduce(_keep_left, points, [])
20
       u = reduce(_keep_left, reversed(points), [])
21
       return l.extend(u[i] for i in range(1, len(u) - 1)) or l
^{22}
                            5.2
                                 Determinant
```

```
def determinant(puntos):
     """Recibe una lista de puntos (tuplas 2D)
2
     v calcula su -determinante-"""
3
     result = 0
4
     size = len(puntos)
5
     for i in range(size):
       x1, x2 = puntos[i][0], puntos[(i+1)%size][0]
       y1, y2 = puntos[i][1], puntos[(i+1)%size][1]
8
9
       result += (x1*y2-x2*y1)
10
11
```

```
return result
```

## 5.3 GreatCircleDistance

```
from math import *

def gratCircleDistance( pLat, pLong, qLat, qLong, radius ):

pLat *= pi/180
pLong *= pi/180
qLat *= pi/180
qLong *= pi/180
return radius*acos(cos(pLat)*cos(pLong)*cos(qLat)*cos(qLong)+
cos(pLat)*sin(pLong)*cos(qLat)*sin(qLong)+
sin(pLat)*sin(qLat))
```

#### 5.4 Perimeter

```
1 | from math import sqrt
  def perimeter(puntos):
     """Recibe una lista de puntos 2D que representan
       los vertices de un poligono y devuelve el perimetro
       del mismo."""
     result = 0
     size = len(puntos)
7
     for i in range(size):
       x1, x2 = puntos[i][0], puntos[(i+1)%size][0]
       y1, y2 = puntos[i][1], puntos[(i+1)%size][1]
       dx, dy = x2-x1, y2-y1
11
       result += sqrt(dx**2+dy**2)
12
13
     return result
```

### 5.5 Turn

```
def turn( p, q, r):
    """Recibe tres puntos p, q y r (2D) y
    devuelve si se encuentran en sentido horario,
    antihorario o alineados"""

result = (r[0]-q[0])*(p[1]-q[1]) - (r[1]-q[1])*(p[0]-q[0])

if(result < 0):</pre>
```

```
return -1 # P->Q->R es una terna derecha (CCW)

if(result > 0):
    return 1 # P->Q->R es una terna izquierda

return 0 # P->Q->R colineales

# Wrapper para chequear directamente CCW, si se toleran colineales usar
    >=

ccw = lambda p, q, r: turn(p, q, r)>0
```

## 6 Strings

#### 6.1 Hash

```
def compute_hash(s):
    p = 31 #Cambiar esto por un primo un poco mas grande
    m = 10**9+9
    p_pow = 1
    hash_value = 0
    for c in s:
        hash_value = (hash_value + (ord(c)-ord('a')+1)*p_pow)%m
        p_pow = (p_pow * p)%m
    return hash_value
```

## 6.2 Prefix Function

```
def prefixFunction(s):
     """Devuelve un array pi, donde pi[i]
     coincide con el mayor prefijo propio que ademas
     es sufijo de s[0...i]"""
    n = len(s)
    pi = [0 for _ in range(n)]
    for i in range(1,n):
       j = pi[i-1]
       while(j>0 and s[i]!=s[j]):
10
         j = pi[j-1]
      if(s[i]==s[j]): j+=1
12
       pi[i] = j
14
15
    return pi
```

#### 6.3 KMP

```
def prefixFunction(s):
    """Devuelve un array pi, donde pi[i]
    coincide con el mayor prefijo propio que ademas
    es sufijo de s[0...i]"""
    n = len(s)
    pi = [0 for _ in range(n)]

for i in range(1,n):
    j = pi[i-1]
    while(j>0 and s[i]!=s[j]):
```

```
j = pi[j-1]
11
       if(s[i]==s[j]): j+=1
12
       pi[i] = j
13
14
     return pi
15
16
   def KMP(s,t):
     """Encuentra todas las ocurrencias de s en t en
18
     O(|s|+|t|)"""
19
     n = len(s); m = len(t)
20
     separator = "#"
21
     #Elegir algun caracter que no este en s ni en t
22
23
     pi = prefixFunction(s+separator+t)
24
     occurences = \Pi
25
26
     for i in range(n+1,n+m+1):
27
       if(pi[i]==n): occurences.append(i-2*n)
28
     return occurences
29
30
   print(prefixFunction("ab#abab"))
  print(KMP("ab", "abab"))
                             6.4 Rabin Karp
   def rabin_karp(s, t):
```

```
"""0(|s|+|t|). Given a pattern s and a text t,
2
     determine if the pattern appears in the text and if it does,
3
     enumerate all its occurrences."""
4
     p = 31
5
     m = 10**9+9
6
     S = len(s); T = len(T)
     p_pow = [1 for _ in range(max(S,T))]
8
     for i in range(1,len(p_pow)):
9
       p_pow[i] = (p_pow[i-1]*p)m
10
     h = [0 \text{ for i in } range(T+1)]
11
     for i in range(T):
^{12}
       h[i+1] = (h[i] + (ord(t[i]) - ord('a') + 1) * p_pow[i]) m
13
     h s = 0
14
     for i in range(S):
15
       h_s = (h_s + (ord(s[i]) - ord('a') + 1) * p_pow[i]) m
16
17
     occurences = []
18
```

```
for i in range(T-S+1):
    cur_h = (h[i+S]-h[i])%m
    if(cur_h == h_s * p_pow[i]%m):
    occurences.append(i)
    return occurences
```

## 6.5 Aplicaciones de KMP y Rabin

```
def prefixFunction(s):
     """Devuelve un array pi, donde pi[i]
     coincide con el mayor prefijo propio que ademas
     es sufijo de s[0...i]"""
     n = len(s)
     pi = [0 for _ in range(n)]
7
     for i in range(1,n):
8
       j = pi[i-1]
9
       while(j>0 and s[i]!=s[j]):
10
         j = pi[j-1]
       if(s[i]==s[j]): j+=1
12
       pi[i] = j
14
     return pi
15
16
   def numOccurencesPrefix(s):
17
     """Cuenta el numero de apariciones de
18
     cada prefijo de s en s"""
19
     pi = prefixFunction(s)
20
     n = len(s)
21
     ans = [0 \text{ for i in } range(n+1)]
22
     for i in range(n):
23
       ans[pi[i]]+=1
24
     i = n-1
25
     while(i>0):
26
       ans[pi[i-1]] += ans[i]
27
       i-=1
28
     for i in range(n+1):
29
       ans[i]+=1
30
     return ans
31
32
   def numDifferentSubstring(s):
33
     """Dada una string s, cuenta la cantidad de
34
     substrings differentes que contiene. O(|s|^2)"""
35
```

```
ans = 1; n = len(s)
for i in range(1,n):
pimax = max(prefixFunction(s[:i+1][::-1]))
ans += i+1-pimax
return ans

6.6 Unique Substrings
| def countUniqueSubstrings(s):
```

```
n = len(s)
2
        p = 31; m = 10**9+9
       p_pow = [1 for _ in range(n)]
5
        for i in range(1,n):
6
            p_pow[i] = (p_pow[i-1]*p)m
7
8
       h = [0 \text{ for i in range}(n+1)]
9
        for i in range(n):
10
            h[i+1] = (h[i]+(ord(s[i])-ord('a')+1) * p_pow[i])/m
11
        cnt = 0
12
        for l in range(1,n+1):
13
            hs = set()
14
            for i in range(n-l+1):
15
                 cur_h = (h[i+1]+m-h[i])%m
16
                 \operatorname{cur}_h = (\operatorname{cur}_h * \operatorname{p-pow}[n-i-1]) \% m
17
                 hs.add(cur_h)
18
            cnt += len(hs)
19
        return cnt
20
  print(countUniqueSubstrings('abcaa'))
```

## 6.7 Group Identical Strings

```
def compute_hash(s):
    p = 31 #Cambiar esto por un primo un poco mas grande
    m = 10**9+9
    p_pow = 1
    hash_value = 0
    for c in s:
        hash_value = (hash_value + (ord(c)-ord('a')+1)*p_pow)%m
        p_pow = (p_pow * p)%m
    return hash_value

def groupIdenticalStrings(s):
```

```
"""Recibo una lista de strings, devuelvo los grupos de strings
12
         identicas
     O(n*m+n*log n) (n=len(s), m = maxlen entre las strings"""
13
14
     hashes = [None for i in range(n)]
15
     for i in range(n):
16
       hashes[i] = (compute_hash(s[i]),i)
17
     hashes.sort()
18
     groups = []
19
     for i in range(n):
       if(i==0 or hashes[i][0] != hashes[i-1][0]):
21
         groups.append([])
22
       groups[-1].append(hashes[i][1])
23
     return groups
24
25
print(groupIdenticalStrings(["aaa", "bca", "aaa", "amclakm"]))
```

## 7 Tricks With Bits

In python3, ~x (flip all bits in other languages) is achieved with (~x & OxFFFFFFFF) (use repit1 lenght of HEXA as you wish)

```
x & (x-1)
clear the lowest set bit of x
x & ~(x-1)
extracts the lowest set bit of x (all others are clear).
Pretty patterns when applied to a linear sequence.
x & (x + (1 << n))
the run of set bits (possibly length 0) starting at bit n cleared.
x \& ^{(x + (1 << n))}
the run of set bits (possibly length 0) in x, starting at bit n.
x \mid (x + 1)
x with the lowest cleared bit set.
x | ^{(x + 1)}
Extracts the lowest cleared bit of x (all others are set),
if "wrapping the expression, you have that cleared value.
x \mid (x - (1 << n))
x With the run of cleared bits (possibly length 0) starting at bit n set.
x \mid (x - (1 << n))
The lowest run of cleared bits (possibly length 0) in x,
starting at bit n are the only clear bits.
```

By 'run' is intended the number formed by all consecutive 1's at the left of n-th bit, starting at n-th bit.

## 3 Plantilla