**數論**

滿足 ceil(*n* / *i*) = *k* 之最大 *i*:

INF, if *k* = 1

*n* / (*k* − 1) − 1, else if *k* − 1 整除 *n*

*n* / (*k* − 1), else

滿足 floor(*n* / *i*) = *k* 之最大 *i*: floor(*n* / *k*)

尤拉函數: phi(*n*) = *n* 乘上所有 (1 − 1/*p*)，對 *n* 之所有質因數 *p*

費馬小定理: *a* \* *a*(*p* − 2) = 1 (mod *p*), *a*, *p* 互質

歐拉降冪公式: *ak* mod *m* = *a* (*k* mod phi(*m*)) mod *m*，其中 gcd(*a*, *m*) = 1

Modulo inverse: inv[i] ≡ -floor(*p* / *i*) × inv[*p* % *i*] (mod *p*)，*p* 為質數。

中國剩餘定理: *x* = *Ai* (mod *mi*), *mi* 兩兩互質，則:

令 *M =* 所有 *mi* 的乘積, *Mi* = *M* / *mi*, *Ti* = *Mi-*1 (mod *mi*), 則 *x* = Σ *Mi* ∙ *Ti* ∙ *Ai* (mod *M*)

枚舉擴展歐幾里得之解:

若 *x*0, *y*0為 *a* ∙ *x* + *b* ∙ *y* = *k* 之一組解，則:

*x* = *x*0 + *t* ∙ *b* / gcd(*a*, *b*), *y* = *y*0 + *t* ∙ *a* / gcd(*a*, *b*) 亦為解，*t* 為整數。

所有互質數加總: Sigma{*i* : gcd(*i*, *n*) = 1 and *i* in [1, *n*]} = *n* ∙ phi(*n*) / 2 for *n* > 1

所有互質數乘積: 一定是 1 或 -1

原根:

1. Exists iff. *n* = 2, 4, *pk* or 2*pk*, where *p* is odd prime.

2. Let *G* be cyclic and *ord*(*G*) = *m*. Then, *g* is a generator of *G* if and only if *gm*/*p*≠ 1 for every prime factor *p* of *m*.

*K*-th root:

*p* is prime and gcd(*k*, *p* − 1) = 1 ==> *k*-th root of *a* = *ax* where *x* is the modulo inverse of *k* modulo *p* − 1.

**排列組合**

**幾何**

三角形 *ABC*，對邊長 *abc*:

海龍公式: triangle area = sqrt(*s*(*s* - *a*)(*s* - *b*)(*s* - *b*)), *s* = 周長 / 2

鞋帶公式: area of simple polygon = ∑{*p*[*i*].*x* × *p*[(*i* + 1) % *n*].*y* − *p*[*i*].*y* × *p*[(*i* + 1) % *n*].*x* }, *p*[0 ... *n* − 1] is an ordered walk.

Pick's Theorem: *A* = *I* + *B*/2 − 1 *I*: interior, *B*: boundary.

正弦定理: *a* / sin*A* = *b* / sin*B* = *c* / sin*C* = 2*R*, *R* 為外接圓半徑

內接圓半徑 = 2 × *area* / (*a* + *b* + *c*)

外接圓半徑 = *abc* / (4 × *area*)

**代數**

若多項式 *f*(*x*) 有有理根 *P*/*Q* (*P*, *Q* 互質)，則 *P* 必為常數項 *a*0 之因數，*Q* 必為領導係數 *an* 之因數。

一矩陣所有 eigen value 之合 = 對角線合。

一矩陣所有 eigen value 之積 = det(*A*)。

特殊等比級數公式: Sigma{*i* ∙ *ri* : *i* in [1, *n*]} = (*n* ∙ *r*(*n* + 1) − *r* ∙ (*rn* − 1) / (*r* − 1)) / (*r* − 1)

**圖論**

平面圖尤拉公式: *V* − *E* + *F* = *C* + 1

最小點覆蓋: 點的集合，所有邊都被覆蓋

最小邊覆蓋: 邊的集合，所有點都被覆蓋

最大獨立集 + 最小點覆蓋 = |*V*|

最大匹配 + 最小邊覆蓋 = |*V*|

最大匹配 = 最大流 (二分圖)

最大匹配 = 最小點覆蓋 (二分圖)

最小點覆蓋 + 最小邊覆蓋 = |*V*| (二分圖)

樹:

對於可以換樹根的樹 以點 1 為準建 LCA: 若 *r* 為當前根，*x*, *y* 為兩點，則新樹中 *x*, *y* 的 LCA 為: lowest vertex({ LCA(*x*, *y*), LCA(*r*, *x*), LCA(*r*, *y*) }) (深度最深)

強連通圖:  
對於任何數 *m*, 如果 *u* 到 *v* 有長度 *x* 的路徑, 則 *v* 到 *u* 有長度 -*x* 的路徑 (mod *m*)

對於任何數 *m* 和一點 *u*, *v*, 一定存在一種方法由 *u* 走到 *v* 再走回 *u*, 且總長度為 *m* 的整數倍

求出 period 的演算法: 建 DFS tree, 令 *p* = 0, 對所有 edge (*s*, *t*), 取 *p* = gcd(*p*, *dep*[*t*] - *dep*[*s*] - *e*.length)

注意: 孤點求出 0, 孤點自環求出 1。

競賽圖:  
Hamilton path 存在 (類似 merge sort *O*(*n* lg *n*)可求)

out-degree 大的點必定可走到 out-degree 小 (或相等) 的點

按照 degree 排 (或先求 Hamilton path), 則 SCC 的編號總是連續

**字串**

*period* *p* > 0: *s*[*i*] = *s*[*i* + *p*]. *proper period*: a period *p* which divides |*s*| and *p* ≠ *s*.

|*s*| − |any proper prefix-suffix| is a period (proper prefix-suffix *k*: *s*[0 ... *k*] = *s*[*n* − *k* ... *n*), *k* < *n*)

Fine and Wilf's Theorem: Suppose that *s* has two periods *p* and *q*. If *p* + *q* − gcd(*p*, *q*) ≤ |*s*|, then gcd(*p*, *q*) is a period of *s*.

Corollaries:

1. For two proper periods *p* and *q*, gcd(*p*, *q*) is a proper period.

2. If *s* has a proper period, then the shortest period is a proper period.

Define *repeat*(*s*) as the string *s*⋅*s*⋅*s*⋅*s*⋅...., which has infinite length (dot = concatenate).

**Lemma**. (folklore) *repeat*(*s*1) < *repeat*(*s*2) if and only if *s*1⋅*s*2 < *s*2⋅*s*1.

**Lemma**. (folklore) *repeat*(*s*1) = *repeat*(*s*2) if and only if *s*1⋅*s*2 = *s*2⋅*s*1.

**Corollary**. (folklore) *repeat*(*s*1) > *repeat*(*s*2) if and only if *s*1⋅*s*2 > *s*2⋅*s*1.

**附錄**

質數 (約 109): 1000000009, 1000000021, 1000000033, 1000000087, 1000000093, 1000000097.

質數 (> 109): 119218851371, 5600748293801, 87178291199.

**General idea**

1. Modulo non-prime: Use CRT. Now mod *pe*.  
 A common approach is to write all numbers in *p-*ary and see how many trailing zeros