

# **ICPC Templates**

我们需要更深入浅出一些

Mine\_King, Tx\_Lcy, 369Pai 洛谷科技

October 30, 2024

# 目录

1	字符	字符串 1						
	1.1	最小表示法						
	1.2	Border 理论						
		1.2.1 关键结论						
		1.2.2 KMP						
	1.3	Z函数						
	1.4	Manacher						
	1.5	AC 自动机						
	1.6	回文自动机 PAM						
	1.7	后缀自动机						
		1.7.1 普通 SAM						
		1.7.2 广义 SAM						
	1.8	后缀排序 7						
2	数据结构							
	2.1	FHQ Treap						
	2.2	K-D Tree						
	2.3	Link Cut Tree						
3	数论 13							
	3.1	Miller Rabin 和 Pollard Rho						
	0.1	3.1.1 Miller Rabin						
		3.1.2 Pollard Rho						
	3.2	常用数论算法						
	J	3.2.1 exgcd						
		3.2.2 CRT						
		3.2.3 exCRT						
		3.2.4 exLucas						
	3.3	万能欧几里得算法						
	3.4	离散对数						
		3.4.1 BSGS						
		3.4.2 exBSGS						

			目录
	3.5	原根	20
		3.5.1 阶	20
		3.5.2 原根	21
	3.6	剩余	22
		3.6.1 二次剩余	23
		3.6.2 Cipolla	23
		3.6.3 模素数 N 次剩余	24
	3.7	min25 筛	24
		3.7.1 简述	24
		3.7.2 求素数个数	25
		3.7.3 完整模板	26
	3.8	组合数的一些有用的公式	27
	3.0		21
4	线性	<b>注代数</b>	31
	4.1	线性空间	31
		4.1.1 正交子空间与正交补	31
	4.2	矩阵	32
		4.2.1 矩阵乘法的另一种理解	32
		4.2.2 基本子空间	32
		4.2.3 高斯消元	32
		4.2.4 逆矩阵	33
	4.3	行列式求值	34
		7732434	
5	图论		36
	5.1	Tarjan	36
		5.1.1 强连通分量	36
		5.1.2 割边与边双	36
		5.1.3 割点与点双	37
	5.2	欧拉路径	38
	5.3	二分图匹配	39
		5.3.1 最大匹配	39
		5.3.2 最大权匹配	39
	5.4	网络流	40
		5.4.1 最大流	40
		5.4.2 费用流	41
		5.4.3 上下界	43
		5.4.4 有负圈的最小费用最大流	44
	5.5	k 短路	44
	5.6	全局最小割	46
	5.7	支配树	47
		2 1/1=1 1	47
	5.8	最大团搜索	49

			目录
	5.9	最小树形图	50
		5.9.1 朱刘算法	50
		5.9.2 可并堆优化	51
	5.10	弦图	53
		5.10.1 MCS 最大势算法。	53
		5.10.2 弦图判定	53
		5.10.3 求弦图的团数与色数	53
		5.10.4 求弦图的最大独立集和最小团覆盖	54
		5.10.5 tricks	54
	5.11	图计数相关	54
		5.11.1 环计数	54
		5.11.2 Prufer 序列	54
6	多项	· 式	56
	6.1	拉格朗日插值法	56
	6.2	牛顿迭代	57
	6.3	FFT	57
	6.4	常用 NTT 模数及其原根	58
	6.5	多项式模板	58
	6.6	FWT	63
7	计算	· ·几何	65
		,	65
8	杂项		72
	8.1		
		8.1.1 splitmix 和仿函数	
		8.1.2 xorshift	73
		8.1.3 手写哈希表	73
	8.2	取模类	74
		8.2.1 Barrett 约减	74
	8.3	快速模乘算法	75
	8.4	常数表	75
	8.5	对拍脚本	76
	8.6	VS Code 配置	76
		8.6.1 User Tasks	76
		8.6.2 设置	77
		8.6.3 快捷键	78

# Chapter 1

# 字符串

## 1.1 最小表示法

```
// == Main ==
int i = 0, j = 1, k = 0;
while (k < n && i < n && j < n)
if (a[(i + k) % n] == a[(j + k) % n]) k++;
else {
    if (a[(i + k) % n] > a[(j + k) % n]) i = i + k + 1;
    else j = j + k + 1;
    if (i == j) i++;
    k = 0;
    ans = min(i, j);
```

## 1.2 Border 理论

### 1.2.1 关键结论

**定理 1**: 对于一个字符串 s,若用 t 表示其最长的 Border,则有  $\mathcal{B}(s) = \mathcal{B}(t) \cup \{t\}$ 。

**定理 2:** 一个字符串的 Border 与 Period 一一对应。具体地, $\operatorname{pre}(s,i) \in \mathcal{B}(s) \iff |s| - i \in \mathcal{P}(s)$ 。

#### 弱周期引理:

$$\forall p,q \in \mathcal{P}(s), p+q \leq |s| \implies \gcd(p,q) \in \mathcal{P}(s)$$

**定理 3**: 若字符串 t 是字符串 s 的前缀,且  $a \in \mathcal{P}(s), b \in \mathcal{P}(t), b \mid a, |t| \geq a$ ,且  $b \in t$  的整周期,则有  $b \in \mathcal{P}(s)$ 。

#### 周期引理:

$$\forall p, q \in \mathcal{P}(s), p + q - \gcd(p, q) \le |s| \implies \gcd(p, q) \in \mathcal{P}(s)$$

**定理 4**: 对于文本串 s 和模式串 t,若  $|t| \ge \frac{|s|}{2}$ ,且 t 在 s 中至少成功匹配了 3 次,则每次匹配的位置形成一个等差数列,且公差为 t 的最小周期。

**定理 5**: 一个字符串 s 的所有长度不小于  $\frac{|s|}{2}$  的 Border 的长度构成一个等差数列。

**定理 6**: 一个字符串的所有 Border 的长度排序后可以划分成  $\lceil \log_2 |s| \rceil$  个连续段,使得每段都是一个等差数列。

定理 7: 回文串的回文前/后缀即为该串的 Border。

**定理 8**: 若回文串 s 有周期 p,则可以把  $\operatorname{pre}(s,p)$  划分成长度为  $|s| \operatorname{mod} p$  的前缀和长度为  $p-|s| \operatorname{mod} p$  的后缀,使得它们都是回文串。

**定理 9**: 若 t 是回文串 s 的最长 Border 且  $|t| \ge \frac{|s|}{2}$ ,则 t 在 s 中只能匹配 2 次。

**定理 10**: 对于任意一个字符串以及  $u,v \in \text{Ssuf}(s), |u| < |v|$ ,一定有  $u \notin v$  的 Border。

**定理 11:** 对于任意一个字符串 s 以及  $u, v \in Ssuf(s), |u| < |v|, 一定有 <math>2|u| \le |v|$ 。

定理 12:  $|\operatorname{Ssuf}(s)| \leq \log_2 |s|$ 。

#### 1.2.2 KMP

### 1.3 Z函数

```
// == Main ==
// n is |s|.
for (int i = 2, j = 0; i <= n; i++) {
    if (i < j + z[j]) z[i] = min(z[i - j + 1], j + z[j] - i);
    while (i + z[i] <= n && s[i + z[i]] == s[1 + z[i]]) z[i]++;
    if (i + z[i] > j + z[j]) j = i;
}
```

#### 1.4 Manacher

```
// == Main ==
// t is the original string, n is |t|.
string s = "^#";
for (char i : t) s.push_back(i), s.push_back('#');
s.push_back ('@');
for (int i = 1, j = 0; i <= 2 * n + 1; i++) {
    if (i <= j + p[j]) p[i] = min (p[2 * j - i], j + p[j] - i);
    while (s[i - p[i] - 1] == s[i + p[i] + 1]) p[i]++;
    if (i + p[i] > j + p[j]) j = i;
}
```

# 1.5 AC 自动机

```
1 // == Preparations ==
2 #include <queue>
3 // == Main ==
4 struct ACAM {
      int tot, fail[200005], delta[200005][26];
      void insert(string s, int id) {
          int now = 0;
          for (char c : s) {
              int v = c - 'a';
              if (!delta[now][v]) delta[now][v] = ++tot;
11
              now = delta[now][v];
          }
13
          return;
14
      void build() {
16
          queue<int> q;
17
          for (int c = 0; c < 26; c++)
```

```
if (delta[0][c]) q.push(delta[0][c]);
19
          while (!q.empty()) {
20
               int now = q.front();
21
               q.pop();
               for (int c = 0; c < 26; c++)
23
                   if (delta[now][c]) fail[delta[now][c]] = delta[fail[now]][c],
24

¬ q.push(delta[now][c]);

                   else delta[now][c] = delta[fail[now]][c];
25
          }
26
          return;
27
      }
29 } ac;
```

# 1.6 回文自动机 PAM

```
1 // == Main ==
2 struct PAM {
      int tot, delta[500005][26], len[500005], fail[500005], ans[500005];
      string s;
      int lst;
      PAM() {tot = 1; len[0] = 0; len[1] = -1; fail[0] = fail[1] = 1;}
      int getfail(int now, int i) {
          while (s[i - len[now] - 1] != s[i]) now = fail[now];
          return now;
10
      }
11
      void insert(int i) {
12
          int now = getfail(lst, i);
13
          if (!delta[now][s[i] - 'a']) {
14
              len[++tot] = len[now] + 2;
15
              fail[tot] = delta[getfail(fail[now], i)][s[i] - 'a'];
              delta[now][s[i] - 'a'] = tot;
17
              ans[tot] = ans[fail[tot]] + 1;
          }
19
          lst = delta[now][s[i] - 'a'];
          return;
      }
22
23 } p;
```

## 1.7 后缀自动机

#### 1.7.1 普通 SAM

```
1 // == Main ==
2 struct SAM {
      int tot, lst;
      int len[2000005], siz[2000005], link[2000005];
      int delta[2000005][26];
      SAM() \{link[0] = -1;\}
      void insert(char ch) {
          int c = ch - 'a', now = ++tot;
          len[now] = len[lst] + 1;
          siz[now] = 1;
11
          for (int p = lst; p != -1; p = link[p])
12
              if (!delta[p][c]) delta[p][c] = tot;
13
              else if (len[delta[p][c]] == len[p] + 1) {link[now] = delta[p][c];
               → break;}
              else {
                   int q = delta[p][c], v = ++tot;
16
                  len[v] = len[p] + 1;
                  memcpy(delta[v], delta[q], sizeof(delta[v]));
18
                   link[v] = link[q], link[q] = v, link[now] = v;
                   for (int i = p; delta[i][c] == q; i = link[i]) delta[i][c] = v;
20
                  break;
21
              }
          lst = now;
23
          return ;
      }
25
26 } sam;
```

### 1.7.2 广义 SAM

注意自动机空间要开 Trie 的两倍。

```
// == Main ==
struct GSAM {
   int tot;
   int delta[2000005][26], link[2000005], len[2000005];
   struct Trie {
      int tot, trie[1000005][26], st[1000005];

   void insert(string s) {
      int now = 0;
      for (char c : s) {
}
```

```
int id = c - 'a';
11
                    if (!trie[now][id]) trie[now][id] = ++tot;
12
                   now = trie[now][id];
13
               }
14
               return;
15
           }
16
      } tr;
17
      GSAM() \{link[0] = -1;\}
19
      int insert(int c, int lst) {
20
           int now = ++tot;
21
           len[now] = len[lst] + 1;
22
           for (int p = lst; p != -1; p = link[p])
23
               if (!delta[p][c]) delta[p][c] = now;
24
               else if (len[delta[p][c]] == len[p] + 1) {link[now] = delta[p][c];
25
                → break;}
               else {
26
                    int q = delta[p][c], v = ++tot;
27
                    len[v] = len[p] + 1;
                    memcpy(delta[v], delta[q], sizeof(delta[v]));
29
                    link[v] = link[q], link[q] = v, link[now] = v;
30
                    for (int i = p; i != -1 && delta[i][c] == q; i = link[i]) delta[i][c]
31
                    \rightarrow = v;
                    break;
32
               }
33
           return now;
34
      }
35
      void build() {
36
           queue<int> q;
37
           tr.st[0] = 0;
38
           q.push(0);
39
           while (!q.empty()) {
40
               int now = q.front();
               q.pop();
42
               for (int i = 0; i < 26; i++)</pre>
43
                    if (tr.trie[now][i])
44
                        tr.st[tr.trie[now][i]] = insert(i, tr.st[now]),
45

¬ q.push(tr.trie[now][i]);

           }
46
           return;
      }
48
49 } gsam;
```

### 1.8 后缀排序

```
1 // == Preparations ==
1 int sa[2000005], rk[2000005], b[1000005], cp[2000005];
3 // == Main ==
4 for (int i = 1; i <= n; i++) b[rk[i] = s[i]]++;</pre>
5 for (int i = 1; i < 128; i++) b[i] += b[i - 1];</pre>
6 for (int i = n; i >= 1; i--) sa[b[rk[i]]--] = i;
7 memcpy(cp, rk, sizeof(cp));
s for (int i = 1, j = 0; i <= n; i++)
      if (cp[sa[i]] == cp[sa[i - 1]]) rk[sa[i]] = j;
      else rk[sa[i]] = ++j;
in for (int w = 1; w < n; w <<= 1) {</pre>
      memcpy(cp, sa, sizeof(cp));
      memset(b, 0, sizeof(b));
13
      for (int i = 1; i <= n; i++) b[rk[cp[i] + w]]++;</pre>
14
      for (int i = 1; i \le n; i++) b[i] += b[i-1];
15
      for (int i = n; i >= 1; i--) sa[b[rk[cp[i] + w]]--] = cp[i];
16
      memcpy(cp, sa, sizeof(cp));
17
      memset(b, 0, sizeof(b));
18
      for (int i = 1; i <= n; i++) b[rk[cp[i]]]++;</pre>
      for (int i = 1; i \le n; i++) b[i] += b[i-1];
20
      for (int i = n; i >= 1; i--) sa[b[rk[cp[i]]]--] = cp[i];
21
      memcpy(cp, rk, sizeof(cp));
22
      for (int i = 1, j = 0; i \le n; i++)
23
          if (cp[sa[i]] == cp[sa[i - 1]] \&\& cp[sa[i] + w] == cp[sa[i - 1] + w])
24
           \rightarrow rk[sa[i]] = j;
          else rk[sa[i]] = ++j;
25
26 }
```

# Chapter 2

# 数据结构

## 2.1 FHQ Treap

```
// == Preparations ==
2 #include <chrono>
3 #include <random>
5 mt19937 gen(chrono::system clock::now().time since epoch().count());
6 // == Main ==
7 struct FHQ Treap {
      struct node {
          int key, val, siz;
          node *ls, *rs;
          node() = default;
12
          node(int key): key( key), val(gen()), siz(1), ls(nullptr), rs(nullptr) {}
          void pushup() {
              siz = 1;
              if (ls) siz += ls->siz;
16
              if (rs) siz += rs->siz;
              return ;
          }
19
      };
20
      node *root;
21
22
      node *merge(node *u, node *v) {
23
          if (!u) return v;
24
          if (!v) return u;
25
          if (u->val < v->val) {u->rs = merge(u->rs, v); u->pushup(); return u;}
          else {v->ls = merge(u, v->ls); v->pushup(); return v;}
27
      }
      void split(node *now, int k, node *&u, node*&v) {
29
          if (!now) {u = v = nullptr; return ;}
          if (now->key < k) u = now, split(now->rs, k, u->rs, v);
```

```
else v = now, split(now->ls, k, u, v->ls);
32
          now->pushup();
33
          return ;
34
      }
      void insert(int k) {
36
          node *u, *v;
          split(root, k, u, v);
38
          root = merge(u, merge(new node(k), v));
          return ;
40
      }
41
      void erase(int k) {
42
          node *u, *v, *w;
43
          split(root, k, u, v), split(v, k + 1, v, w);
44
          node *tmp = v;
          v = merge(v->ls, v->rs);
46
          delete tmp;
47
          root = merge(u, merge(v, w));
48
          return ;
49
      }
      int order_of_key(int k) {
51
          node *u, *v;
52
          split(root, k, u, v);
53
          int ans = u ? u - siz + 1 : 1;
          root = merge(u, v);
55
          return ans;
      }
57
      int find by order(int k) {
          node *now = root;
59
          while (1) {
               int lsiz = now->ls ? now->ls->siz : 0;
               if (lsiz + 1 == k) return now->key;
62
               else if (k <= lsiz) now = now->ls;
63
               else k -= lsiz + 1, now = now->rs;
          }
65
      }
66
      int find_prev(int k) {return find_by_order(order_of_key(k) - 1);}
      int find_next(int k) {return find_by_order(order_of_key(k + 1));}
68
69 } tr;
```

## 2.2 K-D Tree

```
// == Main ==
template<const int Dim = 2>
struct KDTree {
    using point = array<int, Dim>;
struct node {
```

```
point p, l, r;
6
          int val, siz, sum;
          node *ls, *rs;
          node() = default;
10
          node(point _p, int _val = 0):
               p(p), l(p), r(p), val(val), siz(1), sum(val), ls(nullptr),
12

¬ rs(nullptr) {}

          void pushup() {
13
               1 = r = p, siz = 1, sum = val;
               for (int i = 0; i < Dim; i++) {</pre>
                   if (ls) 1[i] = min(1[i], ls->1[i]), r[i] = max(r[i], ls->r[i]);
                   if (rs) l[i] = min(l[i], rs->l[i]), r[i] = max(r[i], rs->r[i]);
17
               }
               if (ls) siz += ls->siz, sum += ls->sum;
19
               if (rs) siz += rs->siz, sum += rs->sum;
20
               return ;
21
          }
22
      };
      vector<node *> root;
24
      using itor = typename vector<node>::iterator;
25
26
      node *build(itor 1, itor r, int dim = 0) {
27
          if (l == r) return nullptr;
28
          int mid = (r - 1) / 2;
          nth element(1, 1 + mid, r, [&dim](const node &x, const node &y) {return
30
           \rightarrow x.p[dim] < y.p[dim];});
          node *now = new node(*(1 + mid));
31
          now->ls = build(l, l + mid, (dim + 1) % Dim);
32
          now->rs = build(1 + mid + 1, r, (dim + 1) % Dim);
33
          now->pushup();
34
          return now;
35
      }
      void getnode(node *now, vector<node> &vec) {
37
          if (!now) return ;
38
          vec.push back(*now);
39
          getnode(now->ls, vec), getnode(now->rs, vec);
          delete now;
          return ;
42
      }
      void insert(point p, int val) {
          vector<node> tmp({node(p, val)});
          while (!root.empty() && root.back()->siz == (int)tmp.size())
46
               getnode(root.back(), tmp), root.pop_back();
          sort(tmp.begin(), tmp.end(), [](const node &x, const node &y) {return x.p <</pre>
48
           \rightarrow y.p;});
          vector<node> vec;
49
          for (node i : tmp)
50
               if (!vec.empty() && vec.back().p == i.p) vec.back().val += i.val;
51
```

```
else vec.push_back(i);
52
          root.push_back(build(vec.begin(), vec.end()));
53
          return ;
      }
      int query(point 11, point rr, node *now) {
56
          if (!now) return 0;
          int flag = 1;
          for (int i = 0; i < Dim; i++)</pre>
               if (now->r[i] < ll[i] || now->l[i] > rr[i]) return 0;
               else flag &= ll[i] <= now->l[i] && now->r[i] <= rr[i];</pre>
          if (flag) return now->sum;
62
          flag = 1;
          for (int i = 0; i < Dim; i++) flag &= ll[i] <= now->p[i] && now->p[i] <=
           → rr[i];
          return flag * now->val + query(11, rr, now->ls) + query(11, rr, now->rs);
65
      }
66
      int query(point 11, point rr) {
67
          int ans = 0;
          for (node *rt : root) ans += query(ll, rr, rt);
          return ans;
70
      }
71
      ~KDTree() {
72
          vector<node> tmp;
          for (node *rt : root) getnode(rt, tmp);
74
      }
75
<sub>76</sub> };
```

### 2.3 Link Cut Tree

代码维护的是点权异或和。

```
1 // == Main ==
2 struct LinkCutTree {
      int fa[100005], son[100005][2], siz[100005], swp[100005];
      int val[100005], Xor[100005];
      void pushup(int now) {
          siz[now] = siz[son[now][0]] + siz[son[now][1]] + 1;
          Xor[now] = Xor[son[now][0]] ^ val[now] ^ Xor[son[now][1]]; // 此处更新信息。
          return;
      }
10
      void pushdown(int now) {
11
          if(!swp[now]) return ;
          swap(son[now][0], son[now][1]);
13
          swp[son[now][0]] ^= 1, swp[son[now][1]] ^= 1;
14
          swp[now] = 0;
15
```

```
// 此处将信息 pushdown
16
          return;
17
      }
18
      int isRoot(int now) {return now != son[fa[now]][0] && now != son[fa[now]][1];}
      int get(int now) {return now == son[fa[now]][1];}
20
      void rotate(int x) {
          int y = fa[x], z = fa[fa[x]], chk = get(x);
22
          if (!isRoot(y)) son[z][get(y)] = x;
23
          son[y][chk] = son[x][chk ^ 1], fa[son[x][chk ^ 1]] = y;
24
          son[x][chk ^ 1] = y, fa[y] = x;
25
          fa[x] = z;
          pushup(y), pushup(x);
27
          return;
28
      }
29
      void splay(int now) {
30
          vector<int> stk;
31
          stk.push back(now);
32
          for (int i = now; !isRoot(i); i = fa[i]) stk.push_back(fa[i]);
33
          while (!stk.empty()) pushdown(stk.back()), stk.pop back();
          for (int f; f = fa[now], !isRoot(now); rotate(now))
35
              if (!isRoot(f)) rotate(get(f) == get(now) ? f : now);
36
          return;
37
      }
      void access(int now) { // 打通到根的链
39
          for (int lst = 0; now; lst = now, now = fa[now]) splay(now), son[now][1] =
          → lst, pushup(now);
          return;
      }
42
      void makeRoot(int now) {access(now); splay(now); swp[now] ^= 1; return;} // 设置
43
      void link(int u, int v) {makeRoot(u); fa[u] = v; return;} // 连接
44
      void cut(int u, int v) {makeRoot(u); access(v); splay(v); son[v][0] = fa[u] = 0;
45
      → return;} // 切割
      int find(int now) { // 找根
46
          access(now), splay(now);
47
          pushdown(now);
48
          while (son[now][0]) now = son[now][0], pushdown(now);
49
          splay(now);
          return now;
51
      }
52
      void split(int u, int v) {makeRoot(u); access(v); splay(u); return;} // 剖出 u ~
53
      v 的链
      void update(int u, int val) {split(u, u); val[u] = Xor[u] = val; return ;} //
54
      → 修改操作,split 后做就行了,此处为单点修改。
      int query(int u, int v) {split(u, v); return Xor[u];} // 查询操作, split 后做就行
55
          了。
      int isConnected(int u, int v) {return find(u) == find(v);} // 查询两个点是否连通。
56
57 };
```

# Chapter 3

# 数论

### 3.1 Miller Rabin 和 Pollard Rho

#### 3.1.1 Miller Rabin

```
1 // == Preparations ==
2 const int prime[] = {2, 3, 5, 7, 9, 11, 13, 17, 19, 23, 29, 31, 37};
4 long long power(long long a, long long b, long long mod) {
      long long ans = 1;
      while (b) {
          if (b & 1) ans = (__int128)ans * a % mod;
          a = (_int128)a * a % mod;
          b >>= 1;
      }
      return ans % mod;
12 }
13 // == Main ==
14 inline int Miller_Rabin(long long n) {
      if (n == 1) return 0;
      if (n == 2) return 1;
      if (n % 2 == 0) return 0;
      long long u = n - 1, t = 0;
      while (u \% 2 == 0) u /= 2, t++;
      for (int i = 0; i < 12; i++) {</pre>
20
          if (prime[i] % n == 0) continue;
          long long x = power(prime[i] % n, u, n);
22
          if (x == 1) continue;
23
          int flag = 0;
          for (int j = 1; j <= t; j++) {
25
              if (x == n - 1) {flag = 1; break;}
26
              x = (_int128)x * x % n;
          if (!flag) return 0;
```

```
30  }
31  return 1;
32 }
```

#### 3.1.2 Pollard Rho

```
1 // == Preparations ==
2 #include <chrono>
3 #include <random>
5 mt19937_64 gen(chrono::system_clock::now().time_since_epoch().count());
6 /*
7 Miller Rabin
8 */
9 // == Main ==
10 long long Pollard Rho(long long n) {
      long long s = 0, t = 0, c = gen() % (n - 1) + 1;
      for (int goal = 1; ; goal <<= 1, s = t) {</pre>
          long long val = 1;
13
          for (int step = 1; step <= goal; step++) {</pre>
14
               t = ((_int128)t * t + c) % n;
15
               val = (_int128)val * abs(t - s) % n;
               if (!val) return n;
               if (step % 127 == 0) {
                   long long d = __gcd(val, n);
19
                   if (d > 1) return d;
               }
          }
22
          long long d = __gcd(val, n);
          if (d > 1) return d;
24
      }
26 }
27 void factor(long long n) {
      if (n < ans) return ;</pre>
      if (n == 1 || Miller Rabin(n)) {
          // n = 1 或 n 是一个质因子。
30
          // ...
31
32
      long long p;
33
      do p = Pollard Rho(n);
34
      while (p == n);
35
      while (n \% p == 0) n /= p;
36
      factor(n), factor(p);
37
      return ;
38
39 }
```

# 3.2 常用数论算法

#### **3.2.1** exgcd

求出来的解满足  $|x| \le b, |y| \le a$ 。

```
// == Main ==
int exgcd(int a, int b, int &x, int &y) {
   if (b == 0) {x = 1; y = 0; return a;}
   int m = exgcd(b, a % b, y, x);
   y -= a / b * x;
   return m;
}
```

#### 3.2.2 CRT

没用。

```
// == Preparations ==
2 #include <vector>
3 // == Main ==
4 int CRT(vector<pair<int, int>> &a) {
5    int M = 1;
6    for (auto i : a) M *= i.second;
7    int res = 0;
8    for (auto i : a) {
9        int t = inv(M / i.second, i.second);
10        res = (res + (long long)i.first * (M / i.second) % M * t % M) % M;
11    }
12    return res;
13 }
```

#### 3.2.3 **exCRT**

需保证 lcm 在 long long 范围内。

```
1 // == Preparations ==
2 long long exgcd(long long a, long long b, long long &x, long long &y);
3 // == Main ==
4 long long exCRT(vector<pair<long long, long long>> vec) {
5 long long ans = vec[0].first, mod = vec[0].second;
6 for (int i = 1; i < (int)vec.size(); i++) {
7 long long a = mod, b = vec[i].second, c = vec[i].first - ans % b;
8 long long x, y;</pre>
```

```
long long g = exgcd(a, b, x, y);
if (c % g != 0) return -1;
b /= g;
x = (__int128)x * (c / g) % b;
ans += x * mod;
mod *= b;
ans = (ans % mod + mod) % mod;
}
return ans;
}
```

#### 3.2.4 exLucas

```
1 // == Preparations ==
2 int power(int a, long long b, int mod);
3 int exgcd(int a, int b, int &x, int &y);
4 int CRT(vector<pair<int, int>> &a);
5 // == Main ==
6 int inv(int n, int p) {
      int x, y;
      exgcd(n, p, x, y);
      return (x % p + p) % p;
10 }
int fac(long long n, int p, int pk) {
      if (n == 0) return 1;
12
      int res = 1;
13
      for (int i = 1; i < pk; i++)</pre>
14
          if (i % p != 0) res = (long long)res * i % pk;
15
      res = power(res, n / pk, pk);
16
      for (int i = 1; i <= n % pk; i++)
17
          if (i % p != 0) res = (long long)res * i % pk;
      return (long long)res * fac(n / p, p, pk) % pk;
19
 }
20
 int C(long long n, long long m, int p, int pk) {
21
      long long x = n, y = m, z = n - m;
22
      int res = (long long)fac(x, p, pk) * inv(fac(y, p, pk), pk) % pk * inv(fac(z, p,
23
      \rightarrow pk), pk) % pk;
      long long e = 0;
24
      while (x) e += x / p, x /= p;
25
      while (y) e -= y / p, y /= p;
26
      while (z) e -= z / p, z /= p;
27
      return (long long)res * power(p, e, pk) % pk;
29 }
 int exLucas(long long n, long long m, int p) {
      vector<pair<int, int>> a;
31
      for (int i = 2; i * i <= p; i++)
          if (p % i == 0) {
33
```

```
int pk = 1;
while (p % i == 0) pk *= i, p /= i;
a.emplace_back(C(n, m, i, pk), pk);

if (p != 1) a.emplace_back(C(n, m, p, p), p);
return CRT(a);

40 }
```

## 3.3 万能欧几里得算法

#### 问题描述:

给出一个幺半群  $(S,\cdot)$  和元素  $u,r \in S$ ,以及一条直线  $y = \frac{ax+b}{c}$ 。

画出平面中所有坐标为正整数的横线和竖线,维护一个 f ,初值为单位元 e 。

从原点出发,先向y轴正方向走直到到达直线与y的交点,然后沿直线走一直走到与x=n的交点为止。

每当经过一条横线时,执行  $f \leftarrow fu$ ,经过一条竖线时执行  $f \leftarrow fr$ 。特别地,在 g 轴上行走时不考虑竖线,同时经过横线和竖线时先执行前者。

求最终的 f。记为 euclid(a, b, c, n, u, r)。

其中  $a, b \ge 0, n, c > 0$ 。

#### 做法:

$$\operatorname{euclid}(a,b,c,n,u,r) = \begin{cases} r^n & m = 0 \\ u^{\lfloor \frac{b}{c} \rfloor} \cdot \operatorname{euclid}(a \bmod c, b \bmod c, c, n, u, u^{\lfloor \frac{a}{c} \rfloor} r) & a \geq c \vee b \geq c \\ r^{\lfloor \frac{c-b-1}{a} \rfloor} u \cdot \operatorname{euclid}(c, (c-b-1) \bmod a, a, m-1, r, u) \cdot r^{n-\lfloor \frac{cm-b-1}{a} \rfloor} & \operatorname{otherwise} \end{cases}$$

设一次乘法的复杂度为O(T),则复杂度为 $O(T\log(a+c)\log(a+n+c))$ 。

```
b >>= 1;
15
      }
16
      return ans;
17
19 Node Euclid(int a, int b, int c, long long n, Node r, Node u) {
      long long m = (a * n + b) / c;
      if (!m) return power(r, n);
21
      if (a >= c || b >= c)
22
           return power(u, b / c) * Euclid(a % c, b % c, c, n, power(u, a / c) * r, u);
23
      return power(r, (c - b - 1) / a) * u *
24
           Euclid(c, (c - b - 1) \% a, a, m - 1, u, r) * power(r, n - (c * m - b - 1) / (c * m - b - 1))
25
26 }
```

## 3.4 离散对数

#### 定义:

取有原根的正整数模数 m ,设其一个原根为 g . 对满足 (a,m)=1 的整数 a ,我们知道必存在 唯一的整数  $0 \le k < \varphi(m)$  使得  $g^k \equiv a \pmod{m}$ 。

我们称这个 k 为以 g 为底,模 m 的离散对数,记作  $k = \text{ind}_{g} a$ 。

离散对数问题即在模p意义下求解 $\log_a b$ 。这等价于求解离散对数方程

$$a^x \equiv b \pmod{p}$$

#### **3.4.1 BSGS**

运用了根号分治的思想: 设块长为  $M \coprod x = AM - B$ ,则有  $a^{AM} \equiv ba^B \pmod p$ 。 固定模数 p 和底数 a 时,预处理时间为  $\mathcal{O}(\frac{p}{M})$ ,单次询问  $\mathcal{O}(M)$  如果数据组数为 T,当 M 取  $\lceil \sqrt{\frac{p}{T}} \rceil$  时取到最优复杂度。 以下代码输入要求  $a \perp p, 2 \leq b, n ,求得的是模意义下 <math>\log_a b$  的最小的非负整数解。

```
1 // == Preparations ==
2 int a , p , m , t , sz , phi;
3 __gnu_pbds::gp_hash_table<int , int>mp;
4 int Qpow(int x , int p , int mod);
5 int Phi(int n);
6 int Inv(int a , int p){return Qpow(a , phi - 1 , p);}
7 // == Main ==
8 void Init()
9 {
10    mp.clear();
11    phi = Phi(p);
```

```
sz = sqrt(phi / m) + 1;
12
      t = ((11)phi + sz - 1) / sz;
13
      int as = \mathbb{Q}pow(a, sz, p), aa = 1;
      for(int i = 1 ; i <= t ; i++)</pre>
           aa = (11)aa * as % p;
           if(!mp[aa])mp[aa] = i;
      }
20 }
21 int BSGS(int b)
      int r = b, ans = p;
23
      for(int k = 0 ; k <= sz ; k++)</pre>
      {
           if(mp.find(r) != mp.end())
26
               ans = min((11)ans, (11)mp[r] * sz - k);
27
           r = (11)r * a % p;
28
29
      return ans >= p ? -1 : ans;
31 }
```

#### **3.4.2 exBSGS**

将方程化为如下形式,其中  $\frac{p}{D} \perp a$ 。

$$\frac{a^k}{D} \cdot a^{x-k} \equiv \frac{b}{D} \pmod{\frac{p}{D}}$$

然后使用 BSGS 求解,注意特判  $x \le k$  的情况。

以下代码输入要求  $1 \le a, p, b \le 10^9$ , 求得的是模意义下  $\log_a b$  的最小的非负整数解。

```
1 // == Preparations ==
1 int a , p , mod , m , t , sz , phi , k , d , inv;
3 __gnu_pbds::gp_hash_table<int , int>mp , low;
4 int Qpow(int x , int p , int mod);
5 int Phi(int n);
6 int Inv(int a , int p);
7 int BSGS(int b);
8 // == Main ==
9 void Init()
10 {
      mp.clear() , low.clear();
11
      a \% = p , mod = p , d = 1 , k = 0;
      int ad = 1 , ak = 1;
13
      for(int g = __gcd(a , p) ; g != 1 ; g = __gcd(a , p))
14
      {
15
          ak = (11)ak * a % mod , k++;
16
```

```
if(!low[ak])low[ak] = k;
17
           d *= g , p /= g , ad = ad * 11(a / g) % p;
18
      }
19
      phi = Phi(p) , inv = Inv(ad , p);
20
      sz = sqrt(phi / m) + 1;
21
      t = ((11)phi + sz - 1) / sz;
22
      int as = Qpow(a , sz , p) , aa = 1;
23
      for(int i = 1 ; i <= t ; i++)</pre>
25
           aa = (11)aa * as % p;
           if(!mp[aa])mp[aa] = i;
27
      }
28
29 }
  int exBSGS(int b)
31 {
      int bm = b % mod;
32
      if(mod == 1 || bm == 1)return 0;
33
      if(low.find(bm) != low.end())return low[bm];
34
      if(b % d)return -1;
      b = (11)(b / d) * inv % p;
36
      int ans = BSGS(b);
37
      return ans == -1 ? -1 : ans + k;
38
39 }
```

## 3.5 原根

### 3.5.1 阶

**定义**: 满足同余式  $a^n \equiv 1 \pmod{m}$  的最小正整数 n 存在,这个 n 称作 a 模 m 的阶,记作  $\delta_m(a)$  或  $\operatorname{ord}_m(a)$ 。

```
性质 1: a, a^2, \dots, a^{\delta_m(a)} 模 m 两两不同余。
```

```
性质 2: 若 a^n \equiv 1 \pmod{m},则 \delta_m(a) \mid n。
```

```
性质 2 推论: 若 a^p \equiv a^q \pmod{m},则有 p \equiv q \pmod{\delta_m(a)}。
```

#### 性质 3:

设 $m \in \mathbf{N}^*$ ,  $a, b \in \mathbf{Z}$ , (a, m) = (b, m) = 1, 则

$$\delta_m(ab) = \delta_m(a)\delta_m(b)$$

的充分必要条件是

$$(\delta_m(a), \delta_m(b)) = 1$$

#### 性质 4:

设 $k \in \mathbb{N}$ ,m为正整数, $a \in \mathbb{Z}$ ,(a, m) = 1,则

$$\delta_m(a^k) = \frac{\delta_m(a)}{(\delta_m(a), k)}$$

#### 3.5.2 原根

#### 定义:

设 m 为正整数, g 为整数。若 (g,m)=1 ,且  $\delta_m(g)=\varphi(m)$  ,则称 g 为模 m 的原根。即 g 满足  $\delta_m(g)=\varphi(m)$ 。当 m 是质数时,我们有  $g^i \mod m, 0 < i < m$  的结果互不相同。

#### 原根判定定理:

设  $m \geq 3, (g,m) = 1$  ,则 g 是模 m 的原根的充要条件是,对于  $\varphi(m)$  的每个素因数 p ,都有  $g^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m}$ 。

#### 原根个数:

若一个数 m 有原根,则它原根的个数为  $\varphi(\varphi(m))$ 。

#### 原根存在定理:

一个数 m 存在原根当且仅当  $m=2,4,p^{\alpha},2p^{\alpha}$  ,其中 p 为奇素数, $\alpha \in \mathbf{N}^*$  。

```
1 // == Preparations ==
2 const int N = 1e6 + 5;
3 int m , pr[N] , phi[N] , vis[N] , mod; bitset<N>b;
4 void Sieve(int n = N - 5);
5 int Qpow(int x , int p , int mod);
6 // == Main ==
7 vector<int> PrimitiveRoot(int p , int d)
8 {
9 vector<int>pfac , g; int mod = p;
```

```
if(!vis[p]){return g;} // whether exist primitive root
10
      for(int i = 1 ; i <= m && pr[i] <= phi[p] ; i++)</pre>
11
          if(phi[p] % pr[i] == 0)pfac.push back(pr[i]);
12
      for(int a = 1; a < p; a++) // minimal primitive root is O(n^{0.25+eps})
13
14
          if(__gcd(a , p) != 1)continue ;
15
          bool ok = 1;
16
          for(int x : pfac)if(Qpow(a , phi[p] / x , mod) == 1){ok = 0; break ;}
          if(!ok)continue;
18
          g.push_back(a); break ;
19
20
      for(int i = 2 ; i < phi[p] ; i++)</pre>
21
          if(\_gcd(i , phi[p]) == 1)g.push_back(Qpow(g[0] , i , mod));
22
      sort(g.begin() , g.end());
23
      return g;
24
25 }
```

### 3.6 剩余

定义: 令整数  $k \geq 2$ ,整数 a ,m 满足 (a,m)=1 ,若存在整数 x 使得  $x^k \equiv a \pmod m \tag{1}$  则称 a 为模 m 的 k 次剩余,否则称 a 为模 m 的 k 次非剩余。

当整数  $k \ge 2$  , 整数 a , m 满足 (a, m) = 1 , 模 m 有原根 g 时,令  $d = (k, \varphi(m))$  , 则:

**性质 1**: a 为模 m 的 k 次剩余当且仅当  $d \mid \operatorname{ind}_g a$  , 即:  $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$ 

```
证明 1: 令 x = g^y ,则方程 (1) 等价于 g^{ky} \equiv g^{\operatorname{ind}_g a} \pmod m

其等价于 ky \equiv \operatorname{ind}_g a \pmod \varphi(m)

由同余的性质,我们知道 y 有整数解当且仅当 d = (k, \varphi(m)) \mid \operatorname{ind}_g a ,进而 a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod m \iff g^{\frac{\varphi(m)}{d} \operatorname{ind}_g a} \equiv 1 \pmod m
\iff \varphi(m) \mid \frac{\varphi(m)}{d} \operatorname{ind}_g a
\iff \varphi(m)d \mid \varphi(m) \operatorname{ind}_g a
\iff d \mid \operatorname{ind}_g a
```

性质 2: 方程 (1) 若有解,则模 m 下恰有 d 个解

**性质 3**: 模 
$$m$$
 的  $k$  次剩余类的个数为  $\frac{\varphi(m)}{d}$  , 其有形式

$$a \equiv g^{di} \pmod{m}, \qquad \left(0 \le i < \frac{\varphi(m)}{d}\right)$$

### 3.6.1 二次剩余

下面讨论模数是奇素数时的二次剩余问题:

$$x^2 \equiv n \pmod{p}$$

参考以上结论不难得出,也就说二次剩余的数量恰为  $\frac{p-1}{2}$  ,其他的非 0 数都是非二次剩余,数量也是  $\frac{p-1}{2}$  ; 判别是否为二次剩余只需检查是否  $n^{\frac{p-1}{2}}\equiv 1\pmod{p}$  即可。

### 3.6.2 Cipolla

通过随机找到一个 a 满足  $a^2 - n$  是非二次剩余。 定义  $i^2 \equiv a^2 - n$ ,将所有数表示为 A + Bi 的形式,有  $(a+i)^{p+1} \equiv n$ 。 那么  $(a+i)^{\frac{p-1}{2}}$  即是一个解,其相反数是另一个解。

```
1 // == Preparations ==
2 typedef long long ll;
3 int mod , w2;
4 mt19937 rnd(114514);
5 struct Complex
6 {
      int a , b;
      Complex(ll aa = 0 , ll bb = 0):a(aa \% mod) , b(bb \% mod){}
9 };
10 typedef Complex cp;
ri cp operator + (cp x , cp y){return cp(x.a + y.a , x.b + y.b);}
12 cp operator - (cp x , cp y){return cp(x.a - y.a , x.b - y.b);}
13 cp operator * (cp x , cp y)
14 {
      return cp((11)x.a * y.a + (11)w2 * x.b % mod * y.b ,
15
                 (11)x.b * y.a + (11)y.b * x.a);
17 }
18 cp Qpow(cp x , int p)
19 {
      cp res = 1;
      while(p)
          if(p \& 1)res = res * x;
23
          x = x * x;
24
```

```
p >>= 1;
25
      }
26
      return res;
27
28 }
29 // == Main ==
30 int Legendre(int a){return Qpow(a , (mod - 1) / 2).a;}
31 pair<int , int> Cipolla(int a)
32 {
      if(a % mod == 0)return {0 , -1};
33
      if(Legendre(a) == mod - 1)return {-1 , -1};
34
      int res = 0;
35
      while(1)
      {
37
           int r = rnd() % mod;
           w2 = ((11)r * r - a) \% mod;
39
           if(w2 < 0)w2 += mod;
           if(w2 == 0)
41
           {
42
               res = r;
               break;
44
           }
45
           if(Legendre(w2) == mod - 1)
           {
               res = \mathbb{Q}pow(cp(r, 1), (mod + 1) / 2).a;
48
               break;
           }
50
51
      if(res * 2 >= mod)res = mod - res;
52
      return {res , mod - res};
53
54 }
```

### 3.6.3 模素数 N 次剩余

我们令  $x = g^c$ ,  $g \not\in p$  的原根(我们一定可以找到这个 g 和 c ),问题转化为求解  $(g^c)^a \equiv b \pmod p$  . 稍加变换,得到

$$(g^a)^c \equiv b \pmod{p}$$

于是就转换成了 BSGS 的基本模型了,可以在  $O(\sqrt{p})$  解出 c ,这样可以得到原方程的一个特解  $x_0 \equiv g^c \pmod{p}$  .

### 3.7 min25 筛

### 3.7.1 简述

应用范围: 求  $\sum_{i=1}^{n} f(i)$ ,其中 f(i) 是积性函数。需要满足 f(i) 在 i 是质数时的取值是多项式。

时间复杂度:  $\Theta(n^{1-\epsilon})/\Theta(\frac{n^{\frac{3}{4}}}{\log n})$ 。

主要想法是将 f(i) 分成三个部分后求和: i 是质数, i 是合数, i=1。

先求出 i 是质数部分的和。

为了方便起见,我们将 f(i) 分解成若干  $x^k$  之和,然后分别计算,这样我们要计算的函数就是**完全 积性函数**了。

考虑埃氏筛的过程,设  $g_{n,k}$  表示**筛了**  $2 \sim n$  中的数,用前 k 个质数来筛,没有被筛掉的数的 f' 值之和。

设  $p_i$  表示第 i 个质数,考虑求出 g 数组,首先容易发现如果  $p_k^2 > n$ ,  $g_{n,k} = g_{n,k-1}$ 。 否则我们会筛掉一些数,由于是完全积性函数,容易得出转移:

$$g_{n,k} = g_{n,k-1} - f'(p_k) \times (g_{\lfloor \frac{n}{p_k} \rfloor, k-1} - \sum_{i=1}^{k-1} f'(p_i))$$

注意 g 数组计算的答案是 "将没被筛掉的数也当成质数"时的答案。

我们考虑计算答案,设  $s_{n,k}$  表示**筛了**  $2 \sim n$  中的数,用前 k 个质数来筛,没有被筛掉的数的 f 值 之和。

现在这个  $s_{n,k}$  求的就是真正的答案了,最终答案就是  $s_{n,0} + f(1)$ 。 设  $sp_i = \sum_{i=1}^i p_i$ , D 为最大的 i 满足  $p_i^2 \le n$ ,容易得出转移:

$$s_{n,k} = g_{n,D} - sp_k + \sum_{p_i^e \le n \& i > k} f(p_i^e) (s_{\frac{n}{p_i^e}, e} + [e > 1])$$

然后暴力递归求出s就行了,不需要记忆化。

#### 

```
1 // == Preparations ==
2 #define int long long
_{3} #define id(x) ((x<=lim)?(id1[x]):(id2[n/(x)]))
4 #define rep(i,j,k) for(int i=j;i<=k;++i)</pre>
5 #define per(i,j,k) for(int i=j;i>=k;--i)
6 int const N=1e6+10;
7 int lim, prime[N], w[N], g[N], id1[N], id2[N], m; bool vis[N];
8 // == Main ==
9 inline void init(){
      //预处理根号以内质数
      rep(i,2,lim){
11
          if (!vis[i]) prime[++prime[0]]=i;
          for (int j=1; j<=prime[0] && i*prime[j]<=lim;++j){</pre>
              vis[i*prime[j]]=1;
14
              if (i%prime[j]==0) break;
          }
16
      }
inline void solve(){
```

```
int n; cin>>n, lim=sqrtl(n), init();
20
      for (int l=1,r;l<=n;l=r+1){</pre>
21
           r=n/(n/1), w[++m]=n/1, g[m]=w[m]-1;
22
           if (w[m] <= lim) id1[w[m]] = m;</pre>
           else id2[n/w[m]]=m;
24
           //预处理 g 数组第一维有可能的取值
      }
26
      rep(i,1,prime[0])
27
           for (int j=1; j<=m && prime[i]*prime[i]<=w[j];++j)</pre>
28
               g[j]-=g[id(w[j]/prime[i])]-(i-1);
29
       cout << g[id(n)] << '\n';
30
31 }
```

### 3.7.3 完整模板

```
1 // == Preparations ==
2 #define int long long
#define rep(i,j,k) for(int i=j;i<=k;++i)</pre>
4 #define per(i,j,k) for(int i=j;i>=k;--i)
s #define id(x) ((x<=lim)?(id1[x]):(id2[n/(x)]))
6 #define add(x,y) (x=((x+y)=mod)?(x+y-mod):(x+y)))
7 // == Main ==
8 //例: 求 f(p^k)=p^k(p^k-1) 的前缀和
,//发现 f(p^k)=p^{2k}-p^k
int const mod=1e9+7;
11 int n;
12 inline int f(int op,int x){
      x\%=mod;
      if (!op) return x;
      return x*x%mod;
15
16 }
inline int F(int x){
      x\%=mod;
      return x*(x-1)%mod;
19
inline int smf(int op,int x){
      x\%=mod;
22
      if (!op) return (x*(x+1)/2)%mod;
23
      return x*(x+1)%mod*(2*x%mod+1)%mod*16666668%mod;
25 }
26 //smf -> f 前缀和
27 int const N=1e6+10;
28 int lim,prime[N],sp1[N],sp2[N],w[N],g1[N],g2[N],id1[N],id2[N],m;bool vis[N];
29 inline void init(){
      //预处理根号以内质数
      rep(i,2,lim){
31
          if (!vis[i]) prime[++prime[0]]=i;
32
```

```
for (int j=1;j<=prime[0] && i*prime[j]<=lim;++j){</pre>
33
               vis[i*prime[j]]=1;
34
               if (i%prime[j]==0) break;
35
           }
      }
37
      rep(i,1,prime[0]){
38
           sp1[i]=sp1[i-1],add(sp1[i],f(0,prime[i]));
39
           sp2[i]=sp2[i-1],add(sp2[i],f(1,prime[i]));
40
      }
41
  }
42
  inline int S(int x,int y){
43
      if (prime[y]>=x) return 0;
44
      int ans=((g2[id(x)]+mod-g1[id(x)])%mod+mod-(sp2[y]-sp1[y]+mod)%mod)%mod;
45
      for (int i=y+1;i<=prime[0] && prime[i]*prime[i]<=x;++i)</pre>
           for (int e=1,gg=prime[i];gg<=x;++e,gg*=prime[i])</pre>
               add(ans,F(gg)*(S(x/gg,i)+(e>1))\mbox{mod});
48
      return ans;
49
 }
50
  inline void solve(){
      cin>>n,lim=sqrtl(n),init();
52
      for (int l=1,r;l<=n;l=r+1){</pre>
53
           r=n/(n/1), w[++m]=n/1;
           g1[m] = (smf(0, w[m]) + mod-1) \%mod;
           g2[m] = (smf(1, w[m]) + mod-1) \%mod;
56
           if (w[m] <= lim) id1[w[m]] = m;</pre>
           else id2[n/w[m]]=m;
58
           //预处理 g 数组第一维有可能的取值
      }
60
      rep(i,1,prime[0])
           for (int j=1;j<=m && prime[i]*prime[i]<=w[j];++j)</pre>
62
               add(g1[j],mod-f(0,prime[i])*(g1[id(w[j]/prime[i])]+mod-sp1[i-1])%mod),
63
               add(g2[j], mod-f(1, prime[i])*(g2[id(w[j]/prime[i]))+mod-sp2[i-1])%mod);
64
      cout << (S(n,0)+1) \mod << ' n';
65
 }
66
```

## 3.8 组合数的一些有用的公式

组合数递推公式 (用途: 求组合数行前缀和):

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$$

范德蒙德卷积:

$$\sum_{i=0}^{k} \binom{n}{i} \binom{m}{k-i} = \binom{n+m}{k}$$

范德蒙德卷积推论 1:

$$\sum_{i=-r}^{s} \binom{n}{r+i} \binom{m}{s-i} = \binom{n+m}{r+s}$$

范德蒙德卷积推论 2:

$$\sum_{i=1}^{n} \binom{n}{i} \binom{n}{i-1} = \binom{2n}{n-1}$$

范德蒙德卷积推论 3:

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}$$

范德蒙德卷积推论 4:

$$\sum_{i=0}^{m} \binom{n}{i} \binom{m}{i} = \binom{n+m}{m}$$

对称恒等式:

$$\binom{n}{m} = \binom{n}{n-m}$$

吸收恒等式:

$$\binom{n}{m} = \frac{n}{m} \binom{n-1}{m-1}$$

不知道叫什么:

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

二项式定理:

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i$$

用来容斥的东西:

$$\sum_{i=0}^{n} (-1)^{i} \binom{n}{i} = [n=0]$$

组合数带权和 (对于  $i^k$  可以得出是关于 n 的 k 次多项式与  $2^{n-k}$  的乘积):

$$\sum_{i=0}^{n} i \binom{n}{i} = n2^{n-1}$$

$$\sum_{i=0}^{n} i^2 \binom{n}{i} = n(n+1)2^{n-2}$$

上指标求和:

$$\sum_{i=m}^{n} \binom{i}{m} = \binom{n+1}{m+1}$$

三项式版恒等式:

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$$

平行恒等式:

$$\sum_{i=0}^{n} \binom{m+i}{i} = \binom{m+n+1}{n}$$

上指标卷积:

$$\sum_{i=0}^{n} \binom{i}{a} \binom{n-i}{b} = \binom{n+1}{a+b+1}$$

二项式反演:

$$f_n = \sum_{i=0}^n \binom{n}{i} g_i \leftrightarrow g_n = \sum_{i=0}^n (-1)^{n-i} \binom{n}{i} f_i$$

$$f_n = \sum_{i=n}^m \binom{i}{n} g_i \leftrightarrow g_n = \sum_{i=n}^m (-1)^{i-n} \binom{i}{n} f_i$$

多项式定理:

设n为正整数, $x_i$ 为实数,则:

其中的  $\binom{n}{n_1,n_2,...,n_t}$  是多重集的排列数,取  $x_1=x_2=...=x_t=1$ ,得到  $\sum \binom{n}{n_1,n_2,...,n_t}=t^n$ 。错位排列:

$$D_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)!$$

卡特兰数:

$$H_n = \frac{1}{n+1} \binom{2n}{n} = \frac{(2n)!}{n!(n+1)!}$$

$$H_n = {2n \choose n} - {2n \choose n-1}$$

$$H_n = \frac{H_{n-1}(4n-2)}{n+1}$$

# Chapter 4

# 线性代数

# 4.1 线性空间

线性空间:给定域 F, F 上的线性空间 V 是一个集合,其上定义了两种二元运算:

• 加法  $+: V \times V \to V$ ;

• 数乘  $\cdot: F \times V \to V$ 。

且满足:

•  $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V, \mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ 

 $(\mathbf{u}, \mathbf{v}, \mathbf{v} \subset \mathbf{v}, \mathbf{u} + (\mathbf{v} + \mathbf{v})) = (\mathbf{u} + \mathbf{v}) + \mathbf{v}$ 

•  $\forall \mathbf{u}, \mathbf{v} \in V, \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ 

•  $\forall \mathbf{v} \in V, \exists -\mathbf{v} \in V, \mathbf{v} + (-\mathbf{v}) = \mathbf{0}$ 

•  $\exists \mathbf{0} \in V, \forall \mathbf{v} \in V, \mathbf{v} + \mathbf{0} = \mathbf{0} + \mathbf{v} = \mathbf{v}$ 

•  $\exists 1 \in F, \forall \mathbf{v} \in V, 1\mathbf{v} = \mathbf{v}$ 

•  $\forall a, b \in F, \mathbf{v} \in V, a(b\mathbf{v}) = (ab)\mathbf{v}$ 

•  $\forall a \in F, \mathbf{u}, \mathbf{v} \in V, a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$ 

•  $\forall a, b \in F, \mathbf{v} \in V, (a+b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$ 

### 4.1.1 正交子空间与正交补

**正交子空间**: 若一个内积空间的子空间 A, B 满足一者中的每个向量都与另一者正交(即内积为 0),那么它们互为正交子空间。

其中内积空间是增添了一个额外的结构(即内积)的向量空间,这里略过其定义,可以狭义地理解为欧几里得空间  $\mathbb{R}^n$ ,内积定义为点积。

**正交补**:对于一个内积空间的子空间 A,若另一个子空间 B 包含所有与子空间 A 正交的向量,则称 B 为 A 的正交补。

## 4.2 矩阵

### 4.2.1 矩阵乘法的另一种理解

- A 右乘矩阵 B,是对 A 的列向量进行线性组合,组合系数记在 B 的每个列向量中。
- B 左乘矩阵 A,是对 B 的行向量进行线性组合,组合系数记在 A 的每个行向量中。

#### 4.2.2 基本子空间

**行空间**: 矩阵 A 的行向量组的生成子空间称为行空间,记为  $C(A^{T})$ 。 **列空间**: 矩阵 A 的列向量组的生成子空间称为列空间,记为 C(A)。

根据矩阵的秩的定义,有:对于任意矩阵 A,有  $\dim C(A^T) = \dim C(A) = \operatorname{rank}(A)$ 。

**零空间:** 矩阵 A 的零空间为 Ax = 0 的所有解构成的空间,记为 N(A)。 **左零空间:** 矩阵 A 的左零空间为  $A^{T}x = 0$ (或表述为  $x^{T}A = 0$ )的所有解构成的空间,记为  $N(A^{T})$ 。

有: 对于任意  $n \times m$  的矩阵 A,有  $\dim N(A) = m - \operatorname{rank}(A)$ , $\dim N(A^{\mathsf{T}}) = n - \operatorname{rank}(A)$ 。

**四个基本子空间的正交性**:根据四个子空间的定义,对于任意矩阵 A 有:

- N(A) 与  $C(A^{T})$  互为正交子空间,且互为正交补。
- $N(A^{\mathsf{T}})$  与 C(A) 互为正交子空间,且互为正交补。

### 4.2.3 高斯消元

```
1 // == Preparations ==
2 double a[M][N];
3 int Cmp(double x , double y = 0){return abs(x - y) < 1e-8 ? 0 : (x < y ? -1 : 1);}
4 // == Main ==
5 int Gauss()
6 {
      int tot = 0;
      for(int i = 1 ; i <= n ; i++)</pre>
          for(int j = tot + 1 ; j <= m ; j++)</pre>
10
           {
11
               if(Cmp(a[j][i]))
12
               {
13
```

```
for(int k = 1; k \le n + 1; k++)
14
                        swap(a[tot + 1][k] , a[j][k]);
15
                   break;
               }
          }
          if(!Cmp(a[tot + 1][i]))continue;
          for(int j = tot + 2; j \le m; j++)
20
          {
               double r = a[j][i] / a[tot + 1][i];
22
               for(int k = 1; k \le n + 1; k++)
23
                   a[j][k] = r * a[tot + 1][k];
          }
25
          tot++;
26
      }
27
      for(int i = tot + 1 ; i <= m ; i++)</pre>
28
      {
29
          if(Cmp(a[i][n + 1]))
30
31
               return -1;// No solutions
          }
33
      }
34
      if(tot == n)
35
      {
          for(int i = n ; i >= 1 ; i--)
37
          {
               a[i][n + 1] /= a[i][i] , a[i][i] = 1;
               for(int j = i - 1; j >= 1; j--)
                   a[j][n + 1] -= a[j][i] * a[i][n + 1] , a[j][i] = 0;
          }
42
          return 0;// One solution
43
44
      return 1;// Many solutions
45
46 }
```

### 4.2.4 逆矩阵

**逆矩阵**: 设 A 是一个 n 阶方阵,若存在 n 阶方阵 B 使得  $AB = BA = I_n$ ,其中  $I_n$  为 n 阶单位矩阵,则称 A 是可逆的,是非奇异矩阵,B 是 A 的逆矩阵,记为  $A^{-1}$ 。否则称 A 不可逆,是奇异矩阵。

逆矩阵可以用来快速求解线性方程组。设有 Ax = b,则有  $x = A^{-1}b$ ,对于不同的 b,每次只需要  $\mathcal{O}(n^2)$  即可计算一组解。这样做的前提是 A 可逆。

```
1 // == Preparations ==
2 const int MOD = 1e9 + 7;
3 int Inv(int x);
```

```
4 // == Main ==
5 bool Inv(int n , int a[N][N * 2])
6 {
      for(int i = 1 ; i <= n ; i++)</pre>
           a[i][i + n] = 1;
      for(int i = 1 ; i <= n ; i++)</pre>
      {
10
           for(int j = i ; j <= n ; j++)</pre>
12
               if(a[j][i] != 0)
               {
                    for(int k = 1; k \le n * 2; k++)
                        swap(a[j][k] , a[i][k]);
16
                    break;
               }
           }
19
           if(!a[i][i])return 0;// No Solution
20
           int inv = Inv(a[i][i]);
21
           for(int j = 1 ; j <= n ; j++)</pre>
23
               if(j == i)continue;
24
               int r = (ll)a[j][i] * inv % MOD;
               for(int k = 1; k \le n * 2; k++)
                    a[j][k] = (a[j][k] - (ll)a[i][k] * r) % MOD;
27
           }
           for(int j = 1; j \le n * 2; j++)
29
               a[i][j] = (ll)a[i][j] * inv % MOD;
      }
31
      for(int i = 1 ; i <= n ; i++)</pre>
32
           for(int j = 1; j <= n; j++)
33
               if(a[i][j + n] < 0)a[i][j + n] += MOD;
34
      return 1;
35
<sub>36</sub> }
```

## 4.3 行列式求值

```
// == Preparations ==
const int N = 605;
// == Main ==
void Swap(int i , int j)
{
    if(i == j)return;
    for(int k = 1 ; k <= n ; k++)
        swap(a[i][k] , a[j][k]);
}
f = -f;
}</pre>
```

```
int Det(int n , int mod , ll a[N][N])
12 {
      int m = 0;
13
      for(int i = 1 ; i <= n ; i++)</pre>
      {
15
           m++;
16
           for(int j = m ; j <= n ; j++)</pre>
17
                if(a[j][i]){Swap(m , j); break ;};
           if(!a[m][i])return 0;
19
           for(int j = m + 1; j \le n; j++)
20
           {
21
                while(a[j][i] && a[m][i])
22
                {
23
                    ll r = a[j][i] / a[m][i] % mod;
                    for(int k = 1 ; k <= n ; k++)</pre>
25
                         a[j][k] = (a[j][k] - (ll)r * a[m][k]) % mod;
                    Swap(m , j);
27
                }
28
                if(!a[m][i])Swap(m , j);
           }
30
       }
31
      ll ans = 1;
32
       for(int i = 1 ; i <= n ; i++)</pre>
33
           ans *= a[i][i];
34
      return (ans * f % mod + mod) % mod;
35
<sub>36</sub> }
```

## Chapter 5

# 图论

## 5.1 Tarjan

#### 5.1.1 强连通分量

```
1 // == Main ==
2 void Tarjan(int now) {
      dfn[now] = low[now] = ++Index;
      s.push(now);
      for (int i = g.hd[now]; i; i = g.nxt[i])
          if (!dfn[g.to[i]]) {
              Tarjan(g.to[i]);
              low[now] = min(low[now], low[g.to[i]]);
          } else if (!scc[g.to[i]]) low[now] = min(low[now], dfn[g.to[i]]);
      if (low[now] == dfn[now]) {
10
          scc cnt++;
11
          for (int x = 0; x != now; s.pop()) {
12
              x = s.top();
13
              scc[x] = scc_cnt;
14
          }
      }
16
      return ;
18 }
```

## 5.1.2 割边与边双

割边:

```
// == Main ==
void Tarjan(int now, int fa) {
    dfn[now] = low[now] = ++Index;
    for (int i = g.hd[now]; i; i = g.nxt[i])
        if (!dfn[g.to[i]]) {
```

```
Tarjan(g.to[i], now);
              low[now] = min(low[now], low[g.to[i]]);
              if (low[g.to[i]] > dfn[now])
                  printf("A Bridge of the Input Garph is (%d, %d)\n", now, g.to[i]);
          } else if (g.to[i] != fa) low[now] = min(low[now], dfn[g.to[i]]);
      return ;
12 }
    边双:
 // == Main ==
 void Tarjan(int now, int fa) {
      dfn[now] = low[now] = ++Index;
      s.push(now);
      for (int i = g.hd[now]; i; i = g.nxt[i])
          if (!dfn[g.to[i]]) {
              Tarjan(g.to[i], now);
              low[now] = min(low[now], low[g.to[i]]);
          } else if (g.to[i] != fa) low[now] = min(low[now], dfn[g.to[i]]);
      if (low[now] == dfn[now]) {
10
          bcc cnt++;
11
          for (int x = 0; x != now; s.pop()) {
12
              x = s.top();
13
              bcc[x] = bcc_cnt;
14
          }
15
      }
16
17
      return ;
18 }
```

#### 5.1.3 割点与点双

割点:

```
1 // == Main ==
2 void Tarjan(int now, int root) {
      dfn[now] = low[now] = ++Index;
      int sons=0, flag=0;
      for (int i=g.hd[now]; i; i = g.nxt[i], sons++)
          if (!dfn[g.to[i]]) {
              Tarjan(g.to[i], now);
              low[now] = min(low[now], low[g.to[i]]);
              if (now!=root && low[g.to[i]] == dfn[now] && !flag)
                  printf("A Cut Vertex of the Input Graph is %d.", now), flag=1;
10
          } else low[now] = min(low[now], dfn[g.to[i]]);
      if (now == root && sons >= 2)
12
          printf("A Cut Vertex of the Input Graph is %d.", now);
13
```

```
return ;
14
15 }
     点双:
1 // == Main ==
2 void Tarjan(int now) {
      dfn[now] = low[now] = ++Index;
      s.push(now);
      for (int i = g.hd[now]; i; i = g.nxt[i], sons++)
          if (!dfn[g.to[i]]) {
              Tarjan(g.to[i]);
              low[now] = min(low[now], low[g.to[i]]);
              if (low[g.to[i]] == dfn[now]) {
                  printf("BCC #%d:\n", ++bcc_cnt);
10
                  for (int x = 0; x != g.to[i]; s.pop())
11
                       printf("%d", x = s.top());
12
                  printf("%d\n", now);
13
              }
          } else low[now] = min(low[now], dfn[g.to[i]]);
15
      return ;
17 }
```

### 5.2 欧拉路径

## 5.3 二分图匹配

#### 5.3.1 最大匹配

```
1 // == Preparations ==
1 int chos[100005], vis[100005];
3 struct graph {/* ... */} g;
4 // == Main ==
5 int dfs(int now) {
      for (int i = g.hd[now]; i; i = g.nxt[i]) {
          if (vis[g.to[i]]) continue;
          vis[g.to[i]] = true;
          if (!chos[g.to[i]] || dfs(chos[g.to[i]])) {
               chos[g.to[i]] = now;
               return 1;
11
          }
12
      }
13
      return 0;
14
15 }
16
17 for (int i = 1; i <= n; i++) {</pre>
      memset(vis, 0, sizeof(vis));
      ans += dfs(i);
19
20 }
```

## 5.3.2 最大权匹配

```
1 // == Preparations ==
1 int vis[1005], mat[1005], pre[1005];
3 long long g[505][1005];
4 long long w[1005], slack[1005];
_5 // edge: g[u][n + v] = w;
6 // == Main ==
7 for (int i = 1; i <= n; i++) {</pre>
      w[i] = ~0x3f3f3f3f3f3f3f3f;
      for (int j = n + 1; j \le n + n; j++) w[i] = max(w[i], (long long)g[i][j]);
10 }
in for (int i = 1; i <= n; i++) {</pre>
      memset(vis, 0, sizeof(vis));
12
      memset(slack, 0x3f, sizeof(slack));
13
      memset(pre, 0, sizeof(pre));
14
      int now = i, ri = 0;
15
      while (1) {
16
          int id = 0;
          long long delta = 0x3f3f3f3f3f3f3f3f3f;
          for (int j = n + 1; j \le n + n; j++)
19
```

```
if (!vis[j]) {
20
                   long long val = w[now] + w[j] - g[now][j];
21
                   if (val < slack[j]) slack[j] = val, pre[j] = ri;</pre>
                   if (slack[j] < delta) delta = slack[j], id = j;</pre>
24
          w[i] -= delta;
           for (int j = n + 1; j \le n + n; j++)
26
               if (vis[j]) w[j] += delta, w[mat[j]] -= delta;
               else slack[j] -= delta;
28
          vis[ri = id] = 1;
           if (mat[ri]) now = mat[ri];
30
           else break;
31
      }
32
      while (ri) {
33
          mat[ri] = mat[pre[ri]];
34
           if (!pre[ri]) {mat[ri] = i; break;}
35
          ri = pre[ri];
36
      }
37
38 }
_{39} long long ans = 0;
40 for (int i = 1; i <= n + n; i++) ans += w[i];
41 printf("%lld\n", ans);
42 for (int i = n + 1; i <= n + n; i++) printf("%d ", mat[i]);
43 puts("");
```

### 5.4 网络流

#### 5.4.1 最大流

```
1 // == Preparations ==
2 #include <queue>
_3 // == Main ==
4 struct Dinic {
      int s, t;
      struct graph {
          int tot, hd[205];
          int nxt[10005], to[10005], dt[10005];
          graph() {tot = 1;}
          void add(int u, int v, int w) {
               nxt[++tot] = hd[u];
11
               hd[u] = tot;
12
               to[tot] = v;
13
               dt[tot] = w;
               return ;
15
          }
16
      } g;
17
```

```
int cur[205], dis[205];
18
19
      void add edge(int u, int v, int f) {g.add(u, v, f), g.add(v, u, 0); return;}
20
      int bfs() {
          memset(dis, 0, sizeof(dis));
22
          queue<int>q;
23
          q.push(s);
24
          dis[s] = 1;
          while (!q.empty()) {
26
               int now = q.front();
               q.pop();
               cur[now] = g.hd[now];
               for (int i = g.hd[now]; i; i = g.nxt[i])
30
                   if (g.dt[i] && !dis[g.to[i]]) dis[g.to[i]] = dis[now] + 1,

¬ q.push(g.to[i]);

          }
32
          return dis[t];
33
      }
34
      long long dinic(int now, long long flow) {
35
          if (now == t) return flow;
36
          long long used = 0;
          for (int i = cur[now]; i && used < flow; i = g.nxt[i])</pre>
               if (g.dt[i] && dis[g.to[i]] == dis[now] + 1) {
                   long long k = dinic(g.to[i], min(flow - used, (long long)g.dt[i]));
40
                   g.dt[i] = k, g.dt[i ^ 1] += k;
                   used += k;
42
                   cur[now] = i;
               }
          if (used == 0) dis[now] = 0;
          return used;
      }
47
      long long solve() {
48
          long long ans = 0;
49
          while (bfs()) ans += dinic(s, 0x3f3f3f3f3f3f3f3f3f);
50
          return ans;
      }
53 } F;
```

#### 5.4.2 费用流

原始对偶:

```
// == Preparations ==
// #include <queue>
// == Main ==
// struct PrimalDual {
// int n, s, t;
```

```
struct graph {
6
          int tot, hd[805];
          int nxt[30005], to[30005], flw[30005], cst[30005];
          graph() {tot = 1;}
10
          void add(int u, int v, int f, int c) {
11
               nxt[++tot] = hd[u];
12
               hd[u] = tot;
               to[tot] = v;
14
               flw[tot] = f;
               cst[tot] = c;
16
               return ;
17
          }
18
      } g;
19
      int h[805], dis[805], f[805], pre[805];
20
      struct node {
21
          int id, val;
22
23
          node() = default;
24
          node(int _id, int _val): id(_id), val(_val) {}
25
          bool operator<(const node &x) const {return val > x.val;}
26
      };
27
      void add_edge(int u, int v, int f, int c) {g.add(u, v, f, c), g.add(v, u, 0, -c);
29

    return;
}
      void spfa() {
30
          queue<int> q;
31
          memset(h, 0x3f, sizeof(h));
32
          h[s] = 0;
33
          q.push(s);
34
          while (!q.empty()) {
35
               int now = q.front();
36
               q.pop();
               f[now] = 0;
               for (int i = g.hd[now]; i; i = g.nxt[i])
39
                   if (g.flw[i] && h[g.to[i]] > h[now] + g.cst[i]) {
40
                       h[g.to[i]] = h[now] + g.cst[i];
                        if (!f[g.to[i]]) q.push(g.to[i]), f[g.to[i]] = 1;
                   }
43
          }
          return ;
45
      }
      int dijkstra() {
47
          priority_queue<node> q;
          memset(dis, 0x3f, sizeof(dis));
49
          memset(pre, 0, sizeof(pre));
          q.emplace(s, dis[s] = 0);
51
          while (!q.empty()) {
52
               int now = q.top().id, tmp = q.top().val;
53
```

```
q.pop();
54
               if (dis[now] != tmp) continue;
55
               for (int i = g.hd[now]; i; i = g.nxt[i])
                   if (g.flw[i] && dis[g.to[i]] > dis[now] + g.cst[i] + h[now] -
                    \rightarrow h[g.to[i]]) {
                        q.emplace(g.to[i], dis[g.to[i]] = dis[now] + g.cst[i] + h[now] -
                        \rightarrow h[g.to[i]]);
                        pre[g.to[i]] = i ^ 1;
                   }
60
           }
          return pre[t];
62
      }
63
      pair<int, int> solve() {
64
           int flow = 0, cost = 0;
           spfa();
           while (dijkstra()) {
67
               for (int i = 1; i <= n; i++)
                   if (dis[i] < 0x3f3f3f3f) h[i] += dis[i];</pre>
               int mnflow = 0x3f3f3f3f;
               for (int i = t; i != s; i = g.to[pre[i]]) mnflow = min(mnflow,
71

    g.flw[pre[i] ^ 1]);

               for (int i = t; i != s; i = g.to[pre[i]]) g.flw[pre[i] ^ 1] -= mnflow,
72

    g.flw[pre[i]] += mnflow;

               flow += mnflow;
73
               cost += mnflow * h[t];
           }
75
          return {flow, cost};
      }
77
78 } F;
```

## 5.4.3 上下界

f(u,v) 表示边 (u,v) 的流量,f(u) 表示 u 的出流减入流,c(u,v) 表示边 (u,v) 的容量。 对于每条边给定一个流量下界 b(u,v),需要额外满足  $\forall (u,v), b(u,v) \leq f(u,v) \leq c(u,v)$ 。

#### 无源汇上下界可行流

没有源点和汇点,对于所有点满足 f(u) = 0,求一个可行的流。 先强制每条边流到流量下界,建立虚拟源汇点 s,t,对于每个点 u 考虑此时的净流量:

- f(u) = 0: 满足条件,不用管。
- f(u) > 0: 出流大于入流,从u向t连容量为f(u)的边。
- f(u) < 0: 入流大于出流,从 $s \in u$  连容量为-f(u)的边。

将原图中每条边的容量设为 c(u,v) - b(u,v),则从 s 到 t 的流相当于增加调整流量的过程。若 s 的出边流满(等同于 t 的入边流满),则找到了一条可行流。

#### 有源汇上下界可行流

连一条 t 到 s 容量正无穷下界为 0 的边,然后跑无源汇上下界可行流即可,流量为新增边的流量。

#### 有源汇上下界最大流

求出可行流后删掉 t 到 s 的边,在残量网络上跑 s 到 t 的最大流,该最大流加上原本的可行流即为答案。

#### 有源汇上下界最小流

同理,改成求 t 到 s 的最大流,原可行流减去该最大流即为答案。

#### 有源汇上下界最小费用流

做法是一样的,所有新增边费用为 0。 需要注意求最小流时需要改成费用最大。

#### 5.4.4 有负圈的最小费用最大流

先钦定所有负圈边流满,即上下界均为流量。然后对于负边建反向、容量相同、费用为相反数的 边用于退流原边。

这样就转化成了有源汇上下界最小费用最大流。

## 5.5 k 短路

复杂度为  $O((n+m)\log n + k\log k)$ 。

```
1 // == Preparations ==
1 int ontree[200005];
3 struct graph {
      int tot, hd[5005];
      int nxt[200005], to[200005];
      long long dt [200005];
      void add(int u, int v, long long w) {
          nxt[++tot] = hd[u];
          hd[u] = tot;
10
          to[tot] = v;
          dt[tot] = w;
12
          return ;
13
      }
14
```

```
15 } g;
16 long long dis[5005];
17 struct node {
      int id;
      long long val;
19
      node() = default;
21
      node(int id, long long val): id( id), val( val) {}
22
      bool operator<(const node &x) const {return val > x.val;}
23
24 };
25 priority queue<node> q;
26 int vis[5005];
28 // 以下左偏树
29 struct HeapNode {
      long long val;
      int to, dist;
31
      HeapNode *ls, *rs;
32
33
      HeapNode() = default;
34
      HeapNode(long long _val, int _to): val(_val), to(_to), dist(1), ls(nullptr),
35

    rs(nullptr) {}
<sub>36</sub> };
37 struct Heap {
      HeapNode *root[5005];
39
      HeapNode *merge(HeapNode *u, HeapNode *v) {
          if (!u) return v;
41
          if (!v) return u;
42
          if (u->val > v->val) swap(u, v);
43
          HeapNode *p = new HeapNode(*u);
44
          p->rs = merge(u->rs, v);
45
          if (!p->ls || p->ls->dist < p->rs->dist) swap(p->ls, p->rs);
          if (p->rs) p->dist = p->rs->dist + 1;
          else p->dist = 1;
          return p;
      }
50
 } h;
52
53 struct Node {
      HeapNode *id;
      long long val;
56
      Node() = default;
      Node(HeapNode * id, long long val): id( id), val( val) {}
58
      bool operator<(const Node &x) const {return val > x.val;}
59
60 };
61 priority_queue<Node> Q;
62 // == Main ==
```

```
63 void dfs(int now) {
      vis[now] = 1;
      for (int i = g.hd[now]; i; i = g.nxt[i])
          if (!vis[g.to[i]] && dis[g.to[i]] == dis[now] + g.dt[i]) ontree[i] = 1,

    dfs(g.to[i]);

      return ;
68 }
69 void dfs2(int now) {
      for (int i = g.hd[now]; i; i = g.nxt[i])
          if (ontree[i]) h.root[g.to[i]] = h.merge(h.root[g.to[i]], h.root[now]),
              dfs2(g.to[i]);
      return;
72
73 }
75 memset(dis, 0x3f, sizeof(dis));
76 q.emplace(n, dis[n] = 0);
  while (!q.empty()) {
      int now = q.top().id;
      long long tmp = q.top().val;
      q.pop();
80
      if (tmp != dis[now]) continue;
81
      for (int i = g.hd[now]; i; i = g.nxt[i])
82
          if (dis[g.to[i]] > dis[now] + g.dt[i]) q.emplace(g.to[i], dis[g.to[i]] =

→ dis[now] + g.dt[i]);
84 }
85 dfs(n);
86 for (int i = 1; i <= n; i++)</pre>
      for (int j = g.hd[i]; j; j = g.nxt[j])
          if (!ontree[j] && g.to[j] != n)
              h.root[g.to[j]] = h.merge(h.root[g.to[j]], new HeapNode(dis[i] + g.dt[j]
               → - dis[g.to[j]], i));
90 dfs2(n);
91 if (h.root[1]) Q.emplace(h.root[1], dis[1] + h.root[1]->val);
  while (!Q.empty()) { // 每次取出来一条路径
      HeapNode *now = Q.top().id;
      long long d = Q.top().val;
94
      Q.pop();
95
      if (now->ls) Q.emplace(now->ls, d - now->val + now->ls->val);
      if (now->rs) Q.emplace(now->rs, d - now->val + now->rs->val);
97
      HeapNode *tmp = h.root[now->to];
      if (tmp) Q.emplace(tmp, d + tmp->val);
99
100 }
```

### 5.6 全局最小割

时间复杂度为 $O(|V|^3)$ 。

```
1 // == Preparations ==
1 int g[605][605], vis1[605], vis2[605];
3 long long w[605];
4 // == Main ==
5 long long Stoer_Wagner() {
      long long ans = 0x3f3f3f3f3f3f3f3f3f;
      for (int i = 1; i < n; i++) {</pre>
          int s = 0, t = 0;
          memset(vis2, 0, sizeof(vis2));
          memset(w, 0, sizeof(w));
          for (int j = 1; j \le n - i + 1; j++) {
11
               int now = 0;
               for (int k = 1; k <= n; k++)</pre>
13
                   if (!vis1[k] && !vis2[k] && w[k] >= w[now]) now = k;
14
               s = t, t = now;
15
               vis2[now] = 1;
               for (int k = 1; k \le n; k++) w[k] += g[k][now];
          ans = min(ans, w[t]);
          vis1[t] = 1;
20
          for (int j = 1; j \le n; j++)
               if (j != s) g[s][j] += g[t][j], g[j][s] += g[j][t];
22
      }
23
      return ans;
24
25 }
```

## 5.7 支配树

 $idom_u$  为 u 在支配树上的父亲。 最后 id 形成 dfs 序。

```
int timer, fa[200005], dfn[200005], id[200005];
int sdom[200005], idom[200005];
17 struct dsu {
      int fa[200005], mn[200005];
19
      dsu() {for (int i = 1; i < 200005; i++) fa[i] = mn[i] = i;}
20
      int find(int x) {
21
           if (x == fa[x]) return x;
22
          int tmp = find(fa[x]);
23
           if (dfn[sdom[mn[fa[x]]]] < dfn[sdom[mn[x]]]) mn[x] = mn[fa[x]];</pre>
24
           return fa[x] = tmp;
25
      }
26
27 } d;
28 vector<int> vec[200005];
29 int siz[200005];
_{30} // == Main ==
 void dfs(int now) {
      id[dfn[now] = ++timer] = now;
      for (int i = g.hd[now]; i; i = g.nxt[i])
33
           if (!dfn[g.to[i]]) fa[g.to[i]] = now, dfs(g.to[i]);
34
      return ;
35
36 }
37 void solve() {
      dfs(1);
38
      for (int i = 1; i <= n; i++) sdom[i] = i;</pre>
      for (int i = timer; i >= 1; i--) {
40
           int u = id[i];
           for (int v : vec[u]) {
42
               d.find(v);
               if (sdom[d.mn[v]] == u) idom[v] = u;
               else idom[v] = d.mn[v];
45
           }
46
           if (i == 1) continue;
           for (int j = fg.hd[u]; j; j = fg.nxt[j]) {
               if (!dfn[fg.to[j]]) continue;
49
               if (dfn[fg.to[j]] < dfn[sdom[u]]) sdom[u] = fg.to[j];</pre>
50
               else if (dfn[fg.to[j]] > dfn[u]) {
51
                   d.find(fg.to[j]);
                   if (dfn[sdom[d.mn[fg.to[j]]]] < dfn[sdom[u]]) sdom[u] =</pre>
53
                        sdom[d.mn[fg.to[j]]];
               }
           }
          vec[sdom[u]].push back(u);
56
           d.fa[u] = fa[u];
      }
58
      for (int i = 2; i <= timer; i++)</pre>
59
           if (idom[id[i]] != sdom[id[i]]) idom[id[i]] = idom[idom[id[i]]];
60
      return ;
61
62 }
```

## 5.8 最大团搜索

给定一张无向图,Bron-Kerbosch 算法可以搜索出所有极大团。其时间复杂度与极大团数量相同,为 $\mathcal{O}(3^{\frac{n}{3}})$ 。

我们定义一张图的 degeneracy 为最小的 d 满足其任意导出子图都存在至少一个点度数  $\leq d$ ,则复杂度为  $\mathcal{O}(dn3^{\frac{d}{3}})$ 。

```
1 // == Preparations ==
2 #define popc __builtin_popcountll
3 typedef long long ll;
_{4} const int N = 55;
s int n , ans , a[N]; ll g[N] , d[N]; //g is graph matrix , b[0...n-1][0...n-1]
6 // == Main ==
7 void Dfs(ll R , ll P , ll X)
8 {
      if(!P)
      {
          if(!X)ans = max(ans , popc(R));//now R is the maximal clique
          return ;
      }
13
      11 v = _-lg(P | X);
      for(ll s = P \hat{} (P & g[v]); s; s -= s & -s)
15
      {
          11 u = lg(s \& -s);
17
          Dfs(R | (111 << u) , P & g[u] , X & g[u]);
          P = 111 << u, X = 111 << u;
19
      }
20
22 void BronKerbosch()
23 {
      for(int i = 0; i < n; i++)d[i] = g[i];
24
      for(int i = 0 ; i < n ; i++)</pre>
      {
          int &k = a[i]; k = -1;
27
          for(int j = 0 ; j < n ; j++)
               if(d[j] != -1 \&\& (k == -1 || popc(d[j]) \le popc(d[k])))
                   k = j;
30
          d[k] = -1;
31
          for(int j = 0 ; j < n ; j++)
32
               if(d[j] >= 0 \&\& (d[j] >> k) \& 1)d[j] ^= 111 << k;
      }
34
      11 P = (111 << n) - 1, X = 0;
35
      for(int i = 0 ; i < n ; i++)</pre>
36
      {
37
```

## 5.9 最小树形图

#### 5.9.1 朱刘算法

基本想法:对除根节点外的所有点,选一条边权最小的入边;对于入边形成的简单环,最多只有一条边会被删除,将环缩成一个点,并改变与其相连边的边权。

如果有环,每轮至少减少一个点。时间复杂度  $\mathcal{O}(nm)$ 。

```
1 bool ZhuLiu(int n , int m , int rt)
2 {
      while(1)
      {
          fill(mn + 1, mn + n + 1, 1e9);
          fill(id + 1, id + n + 1, 0);
          fill(top + 1, top + n + 1, 0);
          for(int i = 1 ; i <= m ; i++)</pre>
          {
               auto [u , v , w] = e[i];
10
               if(w < mn[v])mn[v] = w, fa[v] = u;
          }
12
          for(int i = 1 ; i <= n ; i++)</pre>
               if(i == rt)continue ;
               if(mn[i] != 1e9)ans += mn[i];
16
               else return 0;
          }
          int cnt = 0 , tot = 0;
          for(int i = 1 ; i <= n ; i++)</pre>
20
          {
21
               if(id[i] || i == rt)continue;
22
               int u = i;
23
               for(; u != rt && !top[u] ; u = fa[u])top[u] = i;
24
               if(top[u] == i)
25
               {
                   id[u] = ++cnt;
27
                   for(int v = fa[u] ; v != u ; v = fa[v])
28
                       id[v] = cnt;
               }
31
          if(!cnt)return 1;
32
```

#### 5.9.2 可并堆优化

上述算法的瓶颈在于对每个点(包括缩环得到的点)找边权最小的入边。

考虑用可并堆存储每个点u的入边,为对该点入边边权同时减去w(in(u)),堆需要支持全局减。为了避免每次对没有缩环的点的遍历,将过程改为迭代式的。

同时维护两个并查集,分别记录连通块信息、当前所在环的编号。

为保证图能被缩成一个点,需要先加入边  $(i, i \mod n + 1, +\infty)$ 。

**contraction 树**: 为了计算方案,引入一种树结构,树上的叶子是图的原始节点,每个非叶子节点都表示一个环,每个点的父亲是它所在的环。

收缩过程中,对每个环内的点记录其所在环的编号 f、环上的前驱(即树上的兄弟)pre、以及入边 in,即可刻画出该结构。

由于优化后的缩环过程与r 无关,对于任意合法的根r,都可以通过展开该结构得到以其为根的最小树形图。展开过程:

- 1. 对于任意合法的根节点 r,从 r 开始跳父亲直到 contraction 树的树根。
- 2. 对于每层的环,r 的祖先 u 就是从 r 开始沿树边走,第一个访问到的点,该环不要的边就是  $\operatorname{in}(u)$ 。
- 3. 从  $v = pre_u$  开始依次访问环上的点,跳  $v = pre_v$ ,所有 in(v) 就是环上的边,答案加上 w(in(v))。 根据 v 的入边可以得到进入环 v 的点 p,递归处理 p(即展开环 v),注意 p 只要跳到 v 即可。

展开过程 contraction 树上每条边只会访问一次,是  $\mathcal{O}(n)$  的。

对于缩环过程,可以构造数据,使得 $\mathcal{O}(m)$ 条边需要从堆中 $\operatorname{pop}$ ,时间复杂度 $\mathcal{O}(m \log m)$ 。

```
1 // == Preparations ==
2 #define pre(x) (id[e[in[x]].u])
3 typedef pair<int , int>pr;
4 int n , m , rt , num , h[N] , in[N] , f[N] , pre[N]; ll ans;
5 struct Edge{int u , v , w;}e[M + N];
6 struct Heap<pr>{}pq[N];//mergeable heap
7 struct UnionSet
```

```
8 {
      int fa[N];
      void init(int n){iota(fa + 1 , fa + n + 1 , 1);}
      int find(int x){return x == fa[x] ? x : fa[x] = find(fa[x]);}
      int& operator [](int x){return fa[find(x)];}
 }col , id;
<sub>14</sub> // == Main ==
15 bool Work(int u)
  {
      while(pq[u] && (in[u] = pq[u].top().se , pre(u) == u))
17
          pq[u].pop();
18
      if(!pq[u])return 0;
19
      auto [w, i] = pq[u].top(); int v = pre(u);
20
      in[u] = i , pq[u].tag = w , pq[u].pop();
21
      if(col[u] != col[v])
22
      {
23
          col[u] = col[v];
24
          return 1;
25
      }
      pq[++num].merge(pq[u]), col[u] = col[num];
27
      for(int x = v; x != u; pre[x] = pre(x), x = pre[x])
28
          f[x] = id[x] = num , pq[num].merge(pq[x]);
      f[u] = id[u] = num , pre[u] = v;
      return Work(num);
31
 }
32
33 ll Expand(ll u , ll rt)
34 {
      11 \text{ ans} = 0;
35
      for(; u != rt ; u = f[u])
36
      {
          for(int v = pre[u] ; v != u ; v = pre[v])
          {
39
               int w = e[in[v]].w;
               if(w >= INF)return -1;
               ans += Expand(e[in[v]].v , v) + w;
42
          }
43
      }
44
      return ans;
 }
46
47 ll Solve(int n , int m , int rt , Edge e[N + M])//filled e[1...m]
  {
48
      for(int i = 1; i <= n; i++)e[++m] = {i % n + 1, i, INF};</pre>
      for(int i = 1; i <= m; i++)pq[e[i].v].push(pr(e[i].w, i));</pre>
50
      col.init(n * 2) , id.init(n * 2) , num = n;
      for(int i = 1 ; i <= n ; i++)if(id[i] == i)Work(i);</pre>
52
      return Expand(rt , num);
53
54 }
```

## 5.10 弦图

#### 5.10.1 MCS 最大势算法。

```
1 // == Preparations ==
2 #include <vector>
4 int pos[/* ... */], p[/* ... */];
5 vector<int> vec[/* ... */];
6 // == Main ==
7 for (int i = 1; i <= n; i++) pos[i] = vec[0].size(), vec[0].push_back(i);</pre>
s for (int i = 1, j = 0; i <= n; i++, j++) {
      while (vec[j].empty()) j--;
      int u = p[i] = vec[j].back();
      vec[j].pop back();
11
      pos[u] = -1;
12
      for (int k = g.hd[u]; k; k = g.nxt[k])
13
          if (pos[g.to[k]] != -1) {
14
              int v = g.to[k];
15
              pos[vec[l[v]].back()] = pos[v];
16
               swap(vec[l[v]][pos[v]], vec[l[v]].back());
17
              vec[l[v]].pop back();
18
              pos[v] = vec[++l[v]].size();
19
              vec[l[v]].push back(v);
20
          }
_{23} reverse(p + 1, p + n + 1);
```

### 5.10.2 弦图判定

跑 MCS, 然后判断是否为完美消除序列。

具体地,对于每个  $p_i$ ,找到与之相连且在它之后出现的点,按出现顺序记为  $c_1, c_2, \ldots, c_k$ ,我们只需要判断  $c_1$  与  $c_i$  之间是否有边即可。因为这个团中其他边会在  $p_{c_2}, p_{c_3}, \ldots, p_{c_k}$  中被判断。

## 5.10.3 求弦图的团数与色数

求团数:

设 N(x) 为完美消除序列中在 x 之后且与 x 相连的点的集合,则弦图的最大团一定可以被表示为  $\{x\} + N(x)$ ,则  $|\{x\} + N(x)|$  的最大值就是弦图的团数。

求色数:

考虑按完美消除序列从后往前考虑,贪心染 mex,这样需要的颜色数量等于团数。由于团数小于等于色数,这样取到等号,一定最小。

#### 5.10.4 求弦图的最大独立集和最小团覆盖

最大独立集:

按完美消除序列从前往后贪心。正确性证明:每次考虑最靠前的极大团,选最前面的点不劣于选其他点,且优于不选点。

最小团覆盖:

取最大独立集中的每个点x对应的团 $\{x\}+N(x)$ ,这样需要的团的数量等于最大独立集的大小。由于最大独立集小于等于最小团覆盖,这样取到等号,一定最小。

#### **5.10.5** tricks

区间图是弦图,完美消除序列为按区间右端点从小到大排序。 树上距离不超过 *k* 的点连边是弦图,完美消除序列为 bfs 序的逆序。

## 5.11 图计数相关

#### 5.11.1 环计数

任意环计数: 状压 DP,设  $dp_{S,i}$  为从 S 中最小的点出发,走过的点集为 S,现在在 i 的方案数,在能走到起点时统计答案,最终答案为减去边数再除 2。

三元环计数:将点按度数从小到大排序,然后边从前往后定向,这样每个点出度只有  $O(\sqrt{m})$  条,枚举一个点 u,再枚举 u 指向的点 v,再枚举 v 指向的点 w,check 是否存在边 (u,w) 即可。复杂度分析: 当 v 入度  $\leq \sqrt{m}$  时,u 只有  $O(\sqrt{m})$  个;当 v 入度  $> \sqrt{m}$  时,w 至多  $O(\sqrt{m})$  个。

竞赛图三元环计数:  $\binom{n}{3} - \sum_{i=1}^{n} \binom{d(i)}{2}$ , 其中 d(i) 为 i 的入度或出度。

四元环计数: 同样的方法排序定向,然后枚举一个点a,对所有c记录 $a \rightarrow b \rightarrow c$ 的数量,然后对于每个c任取两个b即可组成一个四元环。

团计数:同样的方法排序定向,然后枚举一个点u,对u 的出边 meet-in-middle。具体来说,对一个集合搜出每个子集是否为团,然后做高维前缀和,枚举另一个集合的子集,维护其是否为团及这个集合中的点与前一个集合中的点的连边的交即可。时间复杂度为 $O(\sqrt{m} \times 2^{\frac{\sqrt{2m}}{2}})$ 。(QOJ7514)

### 5.11.2 Prufer 序列

树到 Prufer 序列的映射:每次选择编号最小的叶子删掉并记录其父亲直到只剩两个点。

```
// == Main ==

2 // d[i] 为 i 的度数 -1

3 for (int i = 1, j = 1; i <= n - 2; i++, j++) {

4    while (d[j]) j++;

5    p[i] = fa[j];

6    while (i <= n - 2 && !--d[p[i]] && p[i] < j) p[i + 1] = fa[p[i]], i++;

7 }
```

Prufer 序列到树的映射: 先算出度数,每次选择一个编号最小的度数为 1 的点与当前 Prufer 序列的点连接,然后给两个点的度数都 -1,最后剩两个度数为 1 的点连起来。

```
1 // == Main ==
2 // d[i] 为 i 的度数 -1
3 p[n - 1] = n;
4 for (int i = 1, j = 1; i < n; i++, j++) {
5     while (d[j]) j++;
6     fa[j] = p[i];
7     while (i < n &&!--d[p[i]] && p[i] < j) fa[p[i]] = p[i + 1], i++;
8 }
```

给一张 k 个连通块的图,每个连通块的点数为  $s_i$ ,求连 k-1 条边使其连通的方案数:

$$\sum_{\substack{d_i \ge 1, \sum_{i=1}^k (d_i - 1) = k - 2}} {k - 2 \choose d_1 - 1, d_2 - 1, \cdots, d_k - 1} \cdot \prod_{i=1}^k s_i^{d_i}$$

$$= \prod_{i=1}^k s_i \sum_{\substack{d_i \ge 1, \sum_{i=1}^k (d_i - 1) = k - 2}} {k - 2 \choose d_1 - 1, d_2 - 1, \cdots, d_k - 1} \cdot \prod_{i=1}^k s_i^{d_i - 1}$$

$$= (\sum_{i=1}^k s_i)^{k-2} \prod_{i=1}^k s_i$$

$$= n^{k-2} \prod_{i=1}^k s_i$$

第二个等号为多元二项式定理。

# Chapter 6

# 多项式

## 6.1 拉格朗日插值法

$$f(k) = \sum_{i=0}^{n} y_i \prod_{j \neq i} \frac{k - x_j}{x_i - x_j}$$

取值连续时的优化:

当  $x_i = i$  时可以优化成 O(n)。

$$f(k) = \sum_{i=0}^{n} y_i \prod_{j \neq i} \frac{k - x_j}{x_i - x_j}$$
$$= \sum_{i=0}^{n} y_i \prod_{j \neq i} \frac{k - j}{i - j}$$

重心拉格朗日插值:

$$f(k) = \sum_{i=0}^{n} y_i \prod_{i \neq j} \frac{k - x_j}{x_i - x_j}$$

$$= \sum_{i=0}^{n} y_i \frac{\prod_{j \neq i} k - x_j}{\prod_{j \neq i} x_i - x_j}$$

$$= \sum_{i=0}^{n} \frac{y_i}{k - x_i} \frac{\prod_{j=0}^{n} k - x_j}{\prod_{j \neq i} x_i - x_j}$$

设 
$$g(k) = \prod_{i=0}^{n} k - x_i, t_i = \frac{y_i}{\prod_{j \neq i} x_i - x_j}$$
。

则

$$f(k) = \sum_{i=0}^{n} \frac{g(k)t_i}{k - x_i}$$
$$= g(k) \sum_{i=0}^{n} \frac{t_i}{k - x_i}$$

于是每次插入只需要更新之前的所有  $t_i$  并计算当前点的  $t_i$  即可,时间复杂度为 O(n)。由于 g(k) 和  $\sum\limits_{i=0}^k \frac{t_i}{k-x_i}$  都可以 O(n) 求得,故询问复杂度也是 O(n)。

## 6.2 牛顿迭代

用于解决下列问题:

已知函数  $G \coprod G(F(x)) = 0$ ,求多项式  $F \pmod{x^n}$ 。

结论:

$$F(x) = F_*(x) - \frac{G(F_*(x))}{G'(F_*(x))} \pmod{x^n}$$

其中  $F_*(x)$  为做到  $x^{n/2}$  时的答案。

#### **6.3** FFT

```
1 // == Preparations ==
 struct complex {
      double a, b;
      complex() = default;
      complex(double _a, double _b): a(_a), b(_b) {}
      complex operator+(const complex &x) const {return complex(a + x.a, b + x.b);}
      complex operator-(const complex &x) const {return complex(a - x.a, b - x.b);}
      complex operator*(const complex &x) const {return complex(a * x.a - b * x.b, a *
      \rightarrow x.b + b * x.a);}
      complex operator/(const complex &x) const {
10
          double t = b * b + x.b * x.b;
          return complex((a * x.a + b * x.b) / t, (b * x.a - a * x.b) / t);
12
      }
      complex &operator+=(const complex &x) {return *this = *this + x;}
14
      complex &operator-=(const complex &x) {return *this = *this - x;}
      complex &operator*=(const complex &x) {return *this = *this * x;}
16
      complex &operator/=(const complex &x) {return *this = *this / x;}
17
```

```
18 };
19 // == Main ==
20 void FFT(vector<complex> &f, int flag) const {
      int n = f.size();
      vector<int> swp(n);
22
      for (int i = 0; i < n; i++) {</pre>
           swp[i] = swp[i >> 1] >> 1 | ((i & 1) * (n >> 1));
24
           if (i < swp[i]) std::swap(f[i], f[swp[i]]);</pre>
26
      for (int mid = 1; mid < n; mid <<= 1) {</pre>
27
           complex w1(cos(pi / mid), flag * sin(pi / mid));
28
           for (int i = 0; i < n; i += mid << 1) {</pre>
               complex w(1, 0);
30
               for (int j = 0; j < mid; j++, w *= w1) {
                    complex x = f[i + j], y = w * f[i + mid + j];
32
                    f[i + j] = x + y, f[i + mid + j] = x - y;
33
               }
34
           }
35
      }
      return;
37
38 }
```

## 6.4 常用 NTT 模数及其原根

模数	原根	分解
167772161	3	$5 \times 2^{25} + 1$
469762049	3	$7 \times 2^{26} + 1$
998244353	3	$119 \times 2^{23} + 1$
1004535809	3	$479 \times 2^{21} + 1$
2013265921	31	$15 \times 2^{27} + 1$
2281701377	3	$17 \times 2^{27} + 1$

## 6.5 多项式模板

```
1 // == Preparations ==
2 #include <vector>
3 // == Main ==
4 namespace Poly {
5    const int mod = 998244353, G = 3, invG = 332748118;
6
7    inline int power(int a, int b) {
8       int ans = 1;
9       while (b) {
10         if (b & 1) ans = (long long)ans * a % mod;
```

```
a = (long long)a * a % mod;
11
               b >>= 1;
12
          }
13
          return ans % mod;
      }
15
16
      struct poly: vector<int> {
17
          poly(initializer list<int> &&arg): vector<int>(arg) {}
          template<typename... argT>
19
          poly(argT &&...args): vector<int>(forward<argT>(args)...) {}
20
21
          poly operator+(const poly &b) const {
22
               const poly &a = *this;
23
               poly ans(max(a.size(), b.size()));
               for (int i = 0; i < (int)ans.size(); i++)</pre>
25
                   ans[i] = ((i < (int)a.size() ? a[i] : 0) + (i < (int)b.size() ? b[i]
26
                    \rightarrow : 0)) % mod;
               return ans;
27
          }
          poly operator+=(const poly &b) {return *this = *this + b;}
29
          poly operator-(const poly &b) const {
30
               const poly &a = *this;
31
               poly ans(max(a.size(), b.size()));
               for (int i = 0; i < (int)ans.size(); i++)</pre>
33
                   ans[i] = ((i < (int)a.size() ? a[i] : 0) - (i < (int)b.size() ? b[i]
                    \rightarrow : 0) + mod) % mod;
               return ans;
          }
36
          poly operator==(const poly &b) {return *this = *this - b;}
          void NTT(poly &g, int flag) const {
               int n = g.size();
39
               vector<unsigned long long> f(g.begin(), g.end());
40
               vector<int> swp(n);
               for (int i = 0; i < n; i++) {
42
                   swp[i] = swp[i >> 1] >> 1 | ((i & 1) * (n >> 1));
43
                   if (i < swp[i]) std::swap(f[i], f[swp[i]]);</pre>
44
               }
45
               for (int mid = 1; mid < n; mid <<= 1) {</pre>
                   int w1 = power(flag ? G : invG, (mod - 1) / mid / 2);
47
                   vector<int> w(mid);
48
                   w[0] = 1;
                   for (int i = 1; i < mid; i++) w[i] = (long long)w[i - 1] * w1 % mod;
                   for (int i = 0; i < n; i += mid << 1)</pre>
51
                        for (int j = 0; j < mid; j++) {
                            int t = (long long)w[j] * f[i + mid + j] % mod;
53
                            f[i + mid + j] = f[i + j] - t + mod;
                            f[i + j] += t;
55
                        }
                   if (mid == 1 << 10)</pre>
57
```

```
for (int i = 0; i < n; i++) f[i] %= mod;</pre>
58
               }
59
               int inv = flag ? 1 : power(n, mod - 2);
               for (int i = 0; i < n; i++) g[i] = f[i] % mod * inv % mod;</pre>
               return;
62
           }
           // 下面是基于转置原理的 NTT, 相对朴素版本效率更高。
           void NTT(poly &g, int flag) const {
66
               int n = g.size();
               vector<int> f(g.begin(), g.end());
               if (flag) {
                    for (int mid = n >> 1; mid >= 1; mid >>= 1) {
70
                        int w1 = power(G, (mod - 1) / mid / 2);
                        vector<int> w(mid);
72
                        w[0] = 1;
73
                        for (int i = 1; i < mid; i++) w[i] = (long long)w[i - 1] * w1 %
74
                        for (int i = 0; i < n; i += mid << 1)</pre>
75
                            for (int j = 0; j < mid; j++) {</pre>
76
                                 int t = (long long)(f[i + j] - f[i + mid + j] + mod) *
77
                                 \rightarrow w[j] % mod;
                                 f[i + j] = f[i + j] + f[i + mid + j] >= mod ?
                                     f[i + j] + f[i + mid + j] - mod : f[i + j] + f[i + j]
79
                                      \rightarrow mid + j];
                                 f[i + mid + j] = t;
80
                            }
                    }
82
                    for (int i = 0; i < n; i++) g[i] = f[i];
               } else {
                    for (int mid = 1; mid < n; mid <<= 1) {</pre>
                        int w1 = power(invG, (mod - 1) / mid / 2);
86
                        vector<int> w(mid);
                        w[0] = 1;
                        for (int i = 1; i < mid; i++) w[i] = (long long)w[i - 1] * w1 %
89
                        \rightarrow mod;
                        for (int i = 0; i < n; i += mid << 1)
                            for (int j = 0; j < mid; j++) {</pre>
                                 int t = (long long)w[j] * f[i + mid + j] % mod;
92
                                 f[i + mid + j] = f[i + j] - t < 0 ? f[i + j] - t + mod :
93
                                 \rightarrow f[i + j] - t;
                                 f[i + j] = f[i + j] + t > = mod ? f[i + j] + t - mod : f[i
                                 \rightarrow + j] + t;
                            }
                    }
                    int inv = power(n, mod - 2);
                    for (int i = 0; i < n; i++) g[i] = (long long)f[i] * inv % mod;
98
               }
               return;
100
```

```
}
101
102
           poly operator*(poly b) const {
103
                poly a(*this);
104
                int n = 1, len = (int)(a.size() + b.size()) - 1;
105
                while (n < len) n <<= 1;
106
                a.resize(n), b.resize(n);
107
                NTT(a, 1), NTT(b, 1);
                poly c(n);
109
                for (int i = 0; i < n; i++) c[i] = (long long)a[i] * b[i] % mod;
                NTT(c, 0);
111
                c.resize(len);
112
                return c;
113
            }
114
           poly operator*=(const poly &b) {return *this = *this * b;}
115
           poly inv() const {
116
                poly f = *this, g;
117
                g.push_back(power(f[0], mod - 2));
118
                int n = 1;
119
                while (n < (int)f.size()) n <<= 1;
120
                f.resize(n << 1);
121
                for (int len = 2; len <= n; len <<= 1) {
122
                     poly tmp(len), ff(len << 1);</pre>
123
                     for (int i = 0; i < len >> 1; i++) tmp[i] = g[i] * 2 % mod;
124
                     for (int i = 0; i < len; i++) ff[i] = f[i];</pre>
125
                     g.resize(len << 1);
126
                    NTT(g, 1), NTT(ff, 1);
                     for (int i = 0; i < len << 1; i++) g[i] = (long long)g[i] * g[i] %
128
                     \rightarrow mod * ff[i] % mod;
                    NTT(g, 0);
129
                     g.resize(len);
130
                     for (int i = 0; i < len; i++) g[i] = (tmp[i] - g[i] + mod) % mod;
131
                }
132
                g.resize(size());
133
                return g;
134
            }
135
           poly sqrt() const { // need F[0] = 1.
136
                poly f = *this, g;
137
                g.push back(1);
138
                int n = 1;
139
                while (n < (int)f.size()) n <<= 1;</pre>
140
                f.resize(n << 1);
                for (int len = 2; len <= n; len <<= 1) {</pre>
142
                    poly tmp(len), ff(len << 1);</pre>
143
                     for (int i = 0; i < len >> 1; i++) tmp[i] = g[i] * 2 % mod;
144
                     for (int i = 0; i < len; i++) ff[i] = f[i];</pre>
                     g.resize(len << 1);</pre>
146
                     NTT(g, 1);
147
```

```
for (int i = 0; i < len << 1; i++) g[i] = (long long)g[i] * g[i] %
148
                      \rightarrow mod;
                     NTT(g, 0);
149
                     g += ff;
150
                     g *= tmp.inv();
151
                     g.resize(len);
152
                 }
153
                g.resize(size());
                 return g;
155
            }
            poly derivative() const {
157
                poly f(*this);
158
                for (int i = 1; i < (int)f.size(); i++) f[i - 1] = (long long)f[i] * i %
159
                 \rightarrow mod;
                f.pop back();
160
                return f;
161
            }
162
            poly integral() const {
163
                poly f(*this);
164
                f.push_back(0);
165
                for (int i = f.size() - 1; i \ge 1; i - - ) f[i] = (long long)f[i - 1] *
166
                 → power(i, mod - 2) % mod;
                f[0] = 0;
167
                return f;
168
            }
169
            poly ln() const {
170
                poly f((derivative() * inv()).integral());
                f.resize(size());
172
                return f;
173
            }
174
            poly exp() const { // 需要满足 F[0] = 0
175
                poly f(*this), g;
176
                g.push_back(1);
                int n = 1;
178
                while (n < (int)size()) n <<= 1;</pre>
179
                 f.resize(n);
180
                for (int len = 2; len <= n; len <<= 1) {</pre>
181
                     poly tmp(g);
182
                     g.resize(len);
183
                     g = g.ln();
184
                     for (int i = 0; i < len; i++) g[i] = (f[i] - g[i] + mod) % mod;
185
                     g[0] = (g[0] + 1) \% mod;
                     g *= tmp;
187
                     g.resize(len);
188
                 }
189
                g.resize(size());
                return g;
191
            }
192
       };
193
```

```
194
       inline poly power(poly f, int b) { // 需要满足 F[0] = 1
195
          f = f.ln();
196
           for (int i = 0; i < (int)f.size(); i++) f[i] = (long long)f[i] * b % mod;
          f = f.exp();
198
          return f;
       }
200
       // 不要求 F[0] = 1 的多项式快速幂
       /*
202
      b1 为指数 mod m, b2 为指数 mod (phi(m) = mod - 1)
203
       如果 b1 传入之前被取模了记得特判 a[0] = 0 且指数 > n 的情况,此时多项式每一位系数都
204
      是 0
      */
205
      poly power(poly f, int b1, int b2 = -1) {
           if (b2 == -1) b2 = b1;
207
           int n = f.size(), p = 0;
208
           reverse(f.begin(), f.end());
209
           while (!f.empty() && !f.back()) f.pop_back(), p++;
210
           if (f.empty() || (long long)p * b1 >= n) return poly(n);
211
           int v = f.back();
212
           int inv = power(v, mod - 2);
213
          for (int &i : f) i = (long long)i * inv % mod;
214
          reverse(f.begin(), f.end());
          f = f.ln();
216
           for (int &i : f) i = (long long)i * b1 % mod;
          f = f.exp();
218
          reverse(f.begin(), f.end());
           for (int i = 1; i <= p * b1; i++) f.push_back(0);</pre>
220
           reverse(f.begin(), f.end());
221
           f.resize(n);
222
           v = power(v, b2);
223
           for (int &i : f) i = (long long)i * v % mod;
224
          return f;
225
      }
226
227 }
```

#### **6.6** FWT

```
8 void FWTand(int a[], int op) {
      for (int 1 = 2; 1 <= n; 1 <<= 1)</pre>
           for (int i = 0; i < n; i += 1)</pre>
               for (int j = 0; j < 1 / 2; j++)
                   a[i + j] = (a[i + j] + (long long)a[i + j + 1 / 2] * op % mod + mod)
12

→ % mod;

      return;
13
14 }
15 void FWTxor(int a[], int op) {
      for (int 1 = 2; 1 <= n; 1 <<= 1)
           for (int i = 0; i < n; i += 1)</pre>
17
               for (int j = 0; j < 1 / 2; j++) {
                   int p = (a[i + j] + a[i + j + 1 / 2]) \% mod, d = (a[i + j] - a[i + j])
19
                    \rightarrow + 1 / 2] + mod) % mod;
                   a[i + j] = (long long)p * op % mod;
20
                   a[i + j + 1 / 2] = (long long)d * op % mod;
21
               }
22
      return;
23
24 }
```

## Chapter 7

# 计算几何

## 7.1 计算几何模板

```
1 // == Preparations ==
2 #include <cmath>
3 #include <chrono>
4 #include <random>
5 #include <vector>
6 #include <algorithm>
7 // == Main ==
8 const double eps = 1e-9;
9 const double pi = acos(-1);
11 // 判断 x < 0 或 x = 0 或 x > 0
12 inline int sign(double x) {return fabs(x) <= eps ? 0 : (x > 0 ? 1 : -1);}
14 // 向量 & 点
15 struct Vect {
      double x, y;
      Vect() = default;
18
      Vect(double _x, double _y): x(_x), y(_y) {}
19
      Vect operator+() const {return *this;}
20
      Vect operator-() const {return Vect(-x, -y);}
21
      Vect operator+(const Vect &b) const {return Vect(x + b.x, y + b.y);}
22
      Vect operator-(const Vect &b) const {return Vect(x - b.x, y - b.y);}
23
      Vect operator*(const double &t) const {return Vect(x * t, y * t);}
24
      Vect operator/(const double &t) const {return Vect(x / t, y / t);}
25
      double operator*(const Vect &b) const {return x * b.x + y * b.y;}
      double operator^(const Vect &b) const {return x * b.y - y * b.x;}
27
      Vect &operator+=(const Vect &b) {return *this = *this + b;}
      Vect &operator-=(const Vect &b) {return *this = *this - b;}
29
      Vect &operator*=(const double &t) {return *this = *this * t;}
      Vect &operator/=(const double &t) {return *this = *this / t;}
```

```
bool operator==(const Vect &b) {return !sign(x - b.x) && !sign(y - b.y);}
32
      double length() const {return sqrt(x * x + y * y);}
      Vect normal() const {return *this / length();}
34
35 };
36 using Point = Vect;
37 // 多边形
38 struct Polygon: vector<Point> {
      Polygon(initializer list<Point> &&arg): vector<Point>(arg) {}
      template<typename... argT>
40
      explicit Polygon(argT &&...args): vector<Point>(forward<argT>(args)...) {}
42
     // 多边形面积
43
      double area() const {
44
          double ans = 0;
          for (int i = 0; i < (int)size(); i++) ans += (*this)[i] ^ (*this)[(i + 1) %

→ size()];
          return ans / 2;
47
      }
48
49 };
50 // 直线
51 struct Line {
     // 表示方式为起点 + 向量
     Point s;
     Vect dir;
     Line() = default;
     Line(Point s, Vect dir): s(s), dir(dir) {}
58 };
59 // 线段
60 struct Segment: Line {
      Segment() = default;
      Segment(Point _s, Vect _dir): Line(_s, _dir) {}
63 };
64 // 圆
65 struct Circle {
     // 表示方式为圆心 + 半径
     Point 0;
67
     double r;
      Circle() = default;
      Circle(Point _0, double _r): 0(_0), r(_r) {}
      double area() {return r * r * pi;}
73 };
75 // 两点的中点
76 inline Point middle(Point a, Point b) {return Point((a.x + b.x) / 2, (a.y + b.y) /
  \rightarrow 2);}
77 // 向量 u 逆时针旋转 rad 后得到的向量
78 inline Vect rotate(Vect u, double rad) {
```

```
return Vect(u.x * cos(rad) - u.y * sin(rad), u.x * sin(rad) + u.y * cos(rad));
80 }
81 // 两点距离
82 inline double dist(Point u, Point v) {return sqrt((u.x - v.x) * (u.x - v.x) + (u.y -
  \rightarrow v.y) * (u.y - v.y));}
83 // 两个向量的夹角
84 inline double angle(Vect a, Vect b) {return atan2(a ^ b, a * b);}
85 // 向量 a 到向量 b 的投影
s6 inline Vect projection(Vect a, Vect b) {return b * (a * b / b.length() /
  → b.length());}
87 // 点 a 到直线 b 的投影
ss inline Point projection(Point a, Line b) {return b.s + projection(a - b.s, b.dir);}
89 // 点 a 关于直线 b 的轴对称点
90 inline Point reflection(Point a, Line b) {return b.s + projection(a - b.s, b.dir) * 2
  → - a:}
91 // 判断两条直线是否平行
92 inline int isParallel(Line a, Line b) {return !sign(a.dir ^ b.dir);}
93 // 判断两条直线是否相交
94 inline int isIntersecting(Line a, Line b) {return !isParallel(a, b);}
95 // 判断两条直线是否垂直
% inline int isOrthogonal(Line a, Line b) {return !sign(a.dir * b.dir);}
97 // 判断点 a 是否在直线 b 上
98 inline int isOnLine(Point a, Line b) {return !sign(b.dir ^ (a - b.s));}
99 // 判断点 a 是否在线段 b 上
inline int isOnSegment(Point a, Segment b) {
      return isOnLine(a, b) && sign((a - b.s) * (a - b.s - b.dir)) \leq 0;
102 }
103 // 判断直线 a 与线段 b 是否相交
  inline int isIntersecting(Line a, Segment b) {
      int va = sign((b.s - a.s) ^ a.dir), vb = sign((b.s + b.dir - a.s) ^ a.dir);
      return !va || !vb || va != vb;
106
  // 判断两条线段是否相交
  inline int isIntersecting(Segment a, Segment b) {
      return isOnSegment(b.s, a) || isOnSegment(b.s + b.dir, a) ||
          isOnSegment(a.s, b) || isOnSegment(a.s + a.dir, b) ||
          (sign((b.s - a.s) ^ a.dir) != sign((b.s + b.dir - a.s) ^ a.dir) \&\&
112
              sign((a.s - b.s) \hat{b.dir}) != sign((a.s + a.dir - b.s) \hat{b.dir}));
114
115 // 直线交点
inline Point intersection(Line a, Line b) {return b.s + b.dir * (a.dir ^ (b.s - a.s))
  → / (b.dir ^ a.dir);}
117 // 点 a 到直线 b 的距离
inline double dist(Point a, Line b) {return dist(a, projection(a, b));}
119 // 点 a 到线段 b 的距离
120 inline double dist(Point a, Segment b) {
      double ans = min(dist(a, b.s), dist(a, b.s + b.dir));
      Point tmp = projection(a, b);
122
      if (isOnSegment(tmp, b)) ans = min(ans, dist(a, tmp));
123
```

```
return ans;
124
125 }
126 // 线段间的距离
  inline double dist(Segment a, Segment b) {
      if (isIntersecting(a, b)) return 0;
      return min({dist(a.s, b), dist(a.s + a.dir, b), dist(b.s, a), dist(b.s + b.dir,
       \rightarrow a)});
130 }
  // 判断多边形是否是凸包
  inline int isConvex(const Polygon &a) {
      int n = a.size();
      for (int i = 0; i < n; i++)</pre>
134
           if (sign((a[(i + 1) % n] - a[i]) ^ (a[(i + 2) % n] - a[i])) < 0) return 0;</pre>
135
      return 1;
136
137
138 // 判断点 a 与多边形 b 的位置关系,返回值: 0 - 在多边形外, 1 - 在多边形边上, 2 - 在多边
   → 形内部
  inline int Containment(Point a, const Polygon &b) {
      int n = b.size(), val = 0;
      for (int i = 0; i < n; i++) {
141
           Segment s = Segment(b[i], b[(i + 1) % n] - b[i]);
142
           if (isOnSegment(a, s)) return 1;
143
           int t = sign((b[(i + 1) \% n] - b[i]) ^ (a - b[i]));
           int va = sign(b[i].y - a.y), vb = sign(b[(i + 1) \% n].y - a.y);
145
           if (t > 0 \&\& va \le 0 \&\& vb > 0) val++;
           if (t < 0 \&\& vb \le 0 \&\& va > 0) val--;
147
148
      return val ? 2 : 0;
149
150 }
  // 点集的凸包
  inline Polygon Andrew(Polygon a) {
      Polygon ans;
153
      sort(a.begin(), a.end(), [](const Point &u, const Point &v) {
154
           return u.x != v.x ? u.x < v.x : u.y < v.y;
155
      });
156
      ans.push_back(a[0]);
157
      for (int i = 1; i < (int)a.size(); i++) {</pre>
158
           while (ans.size() > 1) {
159
               Point tmp = ans.back();
160
               ans.pop back();
161
               if (sign((tmp - ans.back()) ^ (a[i] - tmp)) > 0) {ans.push_back(tmp);
162
               → break;}
163
           ans.push_back(a[i]);
      }
165
      int top = ans.size();
      for (int i = (int)a.size() - 2; i >= 0; i--) {
167
           while ((int)ans.size() > top) {
               Point tmp = ans.back();
169
```

```
ans.pop_back();
170
               if (sign((tmp - ans.back()) ^ (a[i] - tmp)) > 0) {ans.push_back(tmp);
171
                → break;}
           }
           ans.push_back(a[i]);
173
       }
       ans.pop back();
175
       return ans;
176
  // 两个凸包的闵可夫斯基和
  inline Polygon Minkowski(Polygon 1, Polygon r) {
       Polygon diffl, diffr;
       int sizl = l.size(), sizr = r.size();
181
       for (int i = 1; i < sizl; i++) diffl.push_back(l[i] - l[i - 1]);</pre>
182
       for (int i = 1; i < sizr; i++) diffr.push back(r[i] - r[i - 1]);</pre>
183
       Polygon ans;
184
       ans.push back(1[0] + r[0]);
185
       int pl = 0, pr = 0;
186
       while (pl < sizl - 1 && pr < sizr - 1)</pre>
187
           if (sign(diff1[pl] ^ diffr[pr]) < 0) ans.push_back(ans.back() + diff1[pl++]);</pre>
188
           else ans.push back(ans.back() + diffr[pr++]);
189
       while (pl < sizl - 1) ans.push_back(ans.back() + diffl[pl++]);</pre>
190
       while (pr < sizr - 1) ans.push back(ans.back() + diffr[pr++]);</pre>
       return ans;
192
193
  }
  // 旋转卡壳求凸包直径
  inline double Diameter(Polygon a) {
       const int n = a.size();
196
       if (n == 1) return 0;
197
       if (n == 2) return dist(a[0], a[1]);
198
       double ans = 0;
199
       a.push back(a[0]);
200
       for (int i = 0, pos = 2; i < n; i++) {
           Point u = a[i], v = a[i + 1];
202
           ans = max(ans, dist(u, v));
203
           while (sign(((u - a[pos + 1]) ^ (v - a[pos + 1])) - ((u - a[pos]) ^ (v - a[pos + 1])))
204
            \rightarrow a[pos]))) >= 0)
               pos = (pos + 1) \% n;
205
           ans = max({ans, dist(u, a[pos]), dist(v, a[pos])});
206
207
       return ans;
208
209
210 // 扇形面积
inline double sector(double r, double rad) {return r * r * rad / 2;}
212 // 弧度为 rad 的弓形的面积
inline double arch(double r, double rad) {return sector(r, rad) - r * r * sin(rad) /

→ 2;}

214 // 三角形内切圆
215 inline Circle incircle(Point a, Point b, Point c) {
```

```
Line u(a, rotate(b - a, angle(b - a, c - a) / 2)), v(b, rotate(a - b, angle(a - b, angle(b - a, c - a) / 2)), v(b, rotate(b - a, angle(b - a, c - a) / 2)), v(b, rotate(b - a, angle(b - a, c - a) / 2)), v(b, rotate(b - a, angle(b - a, c - a) / 2)), v(b, rotate(b - a, angle(b - a, c - a) / 2)), v(b, rotate(b - a, angle(b - a, c - a) / 2)), v(b, rotate(b - a, angle(b - a, c - a) / 2)), v(b, rotate(b - a, angle(b - a, c - a) / 2)), v(b, rotate(b - a, angle(b - a, c - a) / 2)), v(b, rotate(b - a, angle(b - a, c - a) / 2))), v(b, rotate(b - a, angle(b - a, c - a) / 2))), v(b, rotate(b - a, angle(b - a, c - a) / 2))), v(b, rotate(b - a, angle(b - a, c - a) / 2))), v(b, rotate(b - a, angle(b - a, c - a) / 2))), v(b, rotate(b - a, angle(b - a, c - a) / 2))))
216
          \rightarrow b, c - b) / 2));
          Circle ans;
217
          ans.0 = intersection(u, v);
          ans.r = dist(ans.0, Line(a, b - a));
219
          return ans;
221
222 // 三角形外接圆
   inline Circle circumscribedCircle(Point a, Point b, Point c) {
          Line u(middle(a, b), rotate(b - a, pi / 2)), v(middle(a, c), rotate(c - a, pi /
          \rightarrow 2));
          Circle ans;
225
          ans.0 = intersection(u, v);
226
          ans.r = dist(ans.0, a);
227
          return ans;
228
229 }
   // 最小圆覆盖
   inline Circle minimumCircle(Polygon a) {
          mt19937 gen(chrono::system clock::now().time since epoch().count());
          int n = a.size();
233
          shuffle(a.begin(), a.end(), gen);
234
          Circle ans(Point(0, 0), 0);
235
          for (int i = 0; i < n; i++)</pre>
                if (sign(dist(ans.0, a[i]) - ans.r) > 0) {
237
                      ans = Circle(a[i], 0);
238
                      for (int j = 0; j < i; j++)
239
                            if (sign(dist(ans.0, a[j]) - ans.r) > 0) {
                                  ans = Circle(middle(a[i], a[j]), dist(a[i], a[j]) / 2);
241
                                  for (int k = 1; k < j; k++)
                                        if (sign(dist(ans.0, a[k]) - ans.r) > 0)
243
                                              ans = circumscribedCircle(a[i], a[j], a[k]);
244
                            }
245
                }
246
247
          return ans;
248 }
   // 圆与直线的交点
   inline pair<Point, Point> intersection(Circle a, Line b) {
          Point p = projection(a.0, b);
          double dis = dist(a.0, p);
252
          dis = sqrt(a.r * a.r - dis * dis);
          return {p - b.dir.normal() * dis, p + b.dir.normal() * dis};
254
255 }
   // 两个圆的交点
   inline pair<Point, Point> intersection(Circle a, Circle b) {
          Vect u = b.0 - a.0;
258
         double rad = acos((a.r * a.r + u.length() * u.length() - b.r * b.r) / a.r /
          \rightarrow u.length() / 2);
         u = u.normal() * a.r;
         return {a.0 + rotate(u, rad), a.0 + rotate(u, -rad)};
261
```

```
262 }
263 // 点到圆的切点
  inline pair<Point, Point> tangent(Point a, Circle b) {
       double rad = asin(b.r / dist(b.0, a));
       double dis = dist(b.0, a);
266
      dis = sqrt(dis * dis - b.r * b.r);
      Vect u = (b.0 - a).normal() * dis;
268
      return {a + rotate(u, -rad), a + rotate(u, rad)};
270
  // 两个圆的公切线,返回切点
  inline vector<pair<Point, Point>> commonTangent(Circle a, Circle b) {
       vector<pair<Point, Point>> ans;
       double dis = dist(a.0, b.0);
274
       if (sign(dis - fabs(a.r - b.r)) < 0) return ans;</pre>
275
       else if (sign(dis - fabs(a.r - b.r)) == 0) {
276
           ans.push back(intersection(a, b));
277
           return ans;
278
279
       int flag = 0;
       if (a.r < b.r) swap(a, b), flag = 1;
281
      Vect u = (b.0 - a.0).normal();
       double rad = acos((a.r - b.r) / dis);
283
       ans.emplace back(a.0 + rotate(u, rad) * a.r, b.0 + rotate(-u, rad - pi) * b.r);
       ans.emplace_back(a.0 + rotate(u, -rad) * a.r, b.0 + rotate(-u, pi - rad) * b.r);
285
       if (sign(dis - a.r - b.r) >= 0) {
           rad = acos((a.r + b.r) / dis);
287
           if (sign(rad)) {
               ans.emplace_back(a.0 + rotate(u, rad) * a.r, b.0 + rotate(-u, rad) *
289
                \rightarrow b.r);
               ans.emplace back(a.0 + rotate(u, -rad) * a.r, b.0 + rotate(-u, -rad) *
290
                \rightarrow b.r);
           } else ans.emplace back(a.0 + u * a.r, b.0 - u * b.r);
291
      }
292
       if (flag)
293
           for (auto &i : ans) swap(i.first, i.second);
294
       return ans;
295
296
  // 两个圆的交的面积
  inline double intersectionArea(Circle a, Circle b) {
       int state = commonTangent(a, b).size();
       if (state <= 1) return min(a.area(), b.area());</pre>
300
       if (state >= 3) return 0;
      pair<Point, Point> tmp = intersection(a, b);
302
       double rada = fmod(angle(tmp.second - a.0, tmp.first - a.0) + 2 * pi, 2 * pi);
       double radb = fmod(angle(tmp.first - b.0, tmp.second - b.0) + 2 * pi, 2 * pi);
304
      return arch(a.r, rada) + arch(b.r, radb);
306 }
```

# **Chapter 8**

# 杂项

## 8.1 自定义哈希

## 8.1.1 splitmix 和仿函数

```
1 // == Preparations ==
2 #include <chrono>
3 #include <random>
s mt19937 gen(chrono::system_clock::now().time_since_epoch().count());
6 mt19937_64 genll(chrono::system_clock::now().time_since_epoch().count());
7 // == Main ==
s unsigned splitmix32(unsigned x) {
      unsigned z = (x += 0x9E3779B9);
      z = (z ^ (z >> 16)) * 0x85ebca6b;
      z = (z ^ (z >> 13)) * 0xc2b2ae35;
      return z ^ (z >> 16);
12
13 }
14
unsigned long long splitmix64(unsigned long long x) {
      unsigned long long z = (x += 0x9e3779b97f4a7c15);
      z = (z ^ (z >> 30)) * 0xbf58476d1ce4e5b9;
      z = (z ^ (z >> 27)) * 0x94d049bb133111eb;
      return z \hat{z} > 31;
19
20 }
22 struct custom_hash { // custom hash for unsigned long long
      size_t operator()(unsigned long long x) const {
          return splitmix64(x + genll());
25
<sub>26</sub> };
28 struct custom_hash { // custom hash for pair<unsigned long long, unsigned long long>
      size_t operator()(pair<unsigned long long, unsigned long long> x) const {
```

```
return (splitmix64(x.first + genll()) << 1) ^ splitmix64(x.second + genll());
}
};
```

#### 8.1.2 xorshift

#### 8.1.3 手写哈希表

```
1 // == Main ==
2 template<typename ValType , typename KeyType>
3 struct HashTable
4 {
      static const int M = 13075 , P = 13003; // P < M and P is between N^1.1 to N^1.7
      struct Node{KeyType key; ValType v; int nxt;}e[M];
      int tot , head[P];
      inline void Add(int u , const KeyType& k , const ValType &v){e[++tot] = {k , v ,
      → head[u] } , head[u] = tot;}
      inline int hash(const KeyType& x){return x;}
      ValType& operator[](const KeyType& x)
      {
11
          for(int i = head[hash(x) % P] ; i ; i = e[i].nxt)
12
              if(e[i].key == x)return e[i].v;
13
          Add(hash(x) % P , x , ValType());
14
          return e[tot].v;
15
      }
      ValType at(const KeyType& x)
17
18
          for(int i = head[hash(x) % P] ; i ; i = e[i].nxt)
19
              if(e[i].key == x)return e[i].v;
20
          return ValType();
      }
22
      void clear()
23
      {
          for(int i = 1 ; i <= tot ; i++)</pre>
              head[hash(e[i].key) \% P] = 0 , e[i] = {};
26
          tot = 0;
27
      }
28
29 };
```

## 8.2 取模类

```
1 // == Main ==
2 struct mint {
      static const int mod = 998244353;
      int v;
      mint() = default;
      mint(int v): v(( v % mod + mod) % mod) {}
      explicit operator int() const {return v;}
      mint operator+(const mint &x) const {return v + x.v - (v + x.v < mod ? 0 : mod);}</pre>
      mint &operator+=(const mint &x) {return *this = *this + x;}
10
      mint operator-(const mint &x) const {return v - x.v + (v - x.v >= 0 ? 0 : mod);}
11
      mint &operator-=(const mint &x) {return *this = *this - x;}
12
      mint operator*(const mint &x) const {return (long long)v * x.v % mod;}
13
      mint &operator*=(const mint &x) {return *this = *this * x;}
14
      mint inv() const {
15
          mint a(*this), ans(1);
16
          int b \pmod{-2};
17
          while (b) {
18
              if (b & 1) ans *= a;
              a *= a;
20
              b >>= 1;
          }
22
          return ans;
23
24
      mint operator/(const mint &x) const {return *this * x.inv();}
25
      mint &operator/=(const mint &x) {return *this = *this / x;}
26
      mint operator-() {return mint(-v);}
27
28 };
```

#### 8.2.1 Barrett 约减

当模数不固定时可以加速。

用法:在构造函数中传模数,使用方法为 F.reduce(x),其中 x 是需要取模的数。

```
// == Main ==
struct Barrett {
    unsigned long long b, m;
    Barrett(unsigned long long b = 2): b(b), m((_uint128_t(1) << 64) / b) {}
    unsigned long long reduce(long long x) {
        unsigned long long r = (_uint128_t(x + b) * m) >> 64;
        unsigned long long q = (x + b) - b * r;
        return q >= b ? q - b : q;
}
for a main ==
struct Barrett {
    unsigned long long b = 2): b(b), m((_uint128_t(1) << 64) / b) {}
}
</pre>
```

## 8.3 快速模乘算法

```
// == Preparations ==
2 typedef __float128 f128;
3 typedef __int128 i128;
4 typedef __uint128_t u128;
5 // == Main ==
6 inline i128 mul(i128 x , i128 y , i128 p)
7 {
8     i128 z = (f128) x / p * y;
9     i128 res = (u128)x * y - (u128)z * p;
10    return (res + p) % p;
11
```

## 8.4 常数表

n	$\log_{10} n$	n!	C(n, n/2)	LCM(1n)	$P_n$
2	0.30102999	2	2	2	2
3	0.47712125	6	3	6	3
4	0.60205999	24	6	12	5
5	0.69897000	120	10	60	7
6	0.77815125	720	20	60	11
7	0.84509804	5040	35	420	15
8	0.90308998	40320	70	840	22
9	0.95424251	362880	126	2520	30
10	1	3628800	252	2520	42
11	1.04139269	39916800	462	27720	56
12	1.07918125	479001600	924	27720	77
15	1.17609126	1.31e12	6435	360360	176
20	1.30103000	2.43e18	184756	232792560	627
25	1.39794001	1.55e25	5200300	26771144400	1958
30	1.47712125	2.65e32	155117520	1.444e14	5604
$P_n$	37338 <sub>40</sub>	20422650	966467 <sub>60</sub>	190569292 <sub>100</sub>	1e9 <sub>114</sub>

$n \leq$	10	100	1e3	1e4	1e5	1e6	
$\max \omega(n)$	2	3	4	5	6	7	
$\max d(n)$	4	12	32	64	128	240	
$\pi(n)$	4	25	168	1229	9592	78498	
$n \leq$	1e7	1e8	1e9	1e10	1e11	1e12	
$\max \omega(n)$	8	8	9	10	10	11	
$\max d(n)$	448	768	1344	2304	4032	6720	
$\pi(n)$	664579	5761455	5.08e7	4.55e8	4.12e9	3.7e10	
$n \leq$	1e13	1e14	1e15	1e16	1e17	1e18	
$\max \omega(n)$	12	12	13	13	14	15	
$\max d(n)$	10752	17280	26880	41472	64512	103680	
$\pi(n)$	$\pi(n)$ Prime number theorem: $\pi(x) \sim x/\log(x)$						

## 8.5 对拍脚本

```
#!/usr/bin/bash
    declare -i num=0
    while [ true ]; do
        ./mkdata > in.txt
        time ./mine < in.txt > out.txt
         ./correct < in.txt > ans.txt
        diff out.txt ans.txt
        if [ $? -ne 0 ]; then
10
             echo "WA"
11
             break
12
        fi
13
        num=num+1
14
        echo "Passed $num tests."
15
16
    done
```

## 8.6 VS Code 配置

#### 8.6.1 User Tasks

```
"version": "2.0.0",
4
        "tasks": [
            {
                "type": "shell",
                "label": "My C++ Runner",
                "detail": "Build and Run Current C++ Program",
                "command": [ // 三个编译方式保留一个即可。
10
                    "clear".
                    "&&",
12
                    "g++ ${file} -o ${fileDirname}/${fileBasenameNoExtension}
13
                     → -std=c++14 -Wall -Wextra && echo '== Normal =='",
                     "g++ ${file} -o ${fileDirname}/${fileBasenameNoExtension}
14
                     \rightarrow -std=c++14 -Wall -Wextra -02 && echo '== 02 =='",
                     "g++ ${file} -o ${fileDirname}/${fileBasenameNoExtension}
15
                     → -std=c++14 -Wall -Wextra -fsanitize=undefined,address && echo
                     → '== UB Check =='",
                    "&&",
16
                     "gnome-terminal -- bash -c \"ulimit -s 524288; time
17
                     → ${fileDirname}/${fileBasenameNoExtension}; read -p 'Press ENTER
                     ],
                "problemMatcher": [ // 非必要
19
                    "$gcc"
20
                ],
21
                "group": { // 非必要
22
                    "kind": "build",
23
                     "isDefault": true
24
                },
25
                "presentation": { // 非必要
26
                     "showReuseMessage": false
27
                }
28
            }
29
        ]
30
    }
31
```

### 8.6.2 设置

- 字体大小: 16。("editor.fontSize": 16)
- 添加多个光标的方式: ctrl。("editor.multiCursorModifier": "ctrlCmd")
- 不适用空格代替 Tab。("editor.insertSpaces": false)
- 不允许 Enter 进行代码补全。("editor.acceptSuggestionOnEnter": "off")
- 标尺: 110。("editor.rulers": [110])
- 平滑。("editor.cursorSmoothCaretAnimation": "on")

• 标题栏外观。("window.titleBarStyle": "custom") totally:

```
"editor.fontSize": 16,
"editor.multiCursorModifier": "ctrlCmd",
"editor.insertSpaces": false,
"editor.acceptSuggestionOnEnter": "off",
"editor.rulers": [110],
"editor.cursorSmoothCaretAnimation": "on",
"window.commandCenter": false
}
```

#### 8.6.3 快捷键

- 切换块注释: Ctrl+Shift+A -> Ctrl+Shift+/
- 运行任务: Ctrl+Shift+B -> F11
- 向上移动行: Alt+up -> Ctrl+Shift+up
- 向下移动行: Alt+down -> Ctrl+Shift+down