



# ICPC Templates

我们需要更深入浅出一些

Mine\_King, Tx\_Lcy, 369pai

洛谷科技

October 28, 2024

# 目录

<b>1</b>	<b>字符串</b>	<b>1</b>
1.1	最小表示法	1
1.2	Border 理论	1
1.2.1	关键结论	1
1.2.2	KMP	2
1.3	Z 函数	3
1.4	Manacher	3
1.5	AC 自动机	3
1.6	回文自动机 PAM	4
1.7	后缀自动机	5
1.7.1	普通 SAM	5
1.7.2	广义 SAM	5
1.8	后缀排序	7
<b>2</b>	<b>数据结构</b>	<b>8</b>
2.1	FHQ Treap	8
2.2	K-D Tree	9
2.3	Link Cut Tree	11
<b>3</b>	<b>数论</b>	<b>13</b>
3.1	Miller Rabin 和 Pollard Rho	13
3.1.1	Miller Rabin	13
3.1.2	Pollard Rho	14
3.2	常用数论算法	15
3.2.1	exgcd	15
3.2.2	CRT	15
3.2.3	exCRT	15
3.2.4	exLucas	16
3.3	万能欧几里得算法	17
3.4	离散对数	18
3.4.1	BSGS	18
3.4.2	exBSGS	19

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
<b>4</b>	<b>线性代数</b>	<b>28</b>
4.1	行列式求值 . . . . .	28
<b>5</b>	<b>图论</b>	<b>30</b>
5.1	Tarjan . . . . .	30
5.1.1	强连通分量 . . . . .	30
5.1.2	割边与边双 . . . . .	30
5.1.3	割点与点双 . . . . .	31
5.2	欧拉路径 . . . . .	32
5.3	二分图匹配 . . . . .	33
5.3.1	最大匹配 . . . . .	33
5.3.2	最大权匹配 . . . . .	33
5.4	网络流 . . . . .	34
5.4.1	最大流 . . . . .	34
5.4.2	费用流 . . . . .	35
5.4.3	上下界 . . . . .	37
5.4.4	有负圈的最小费用最大流 . . . . .	38
5.5	k 短路 . . . . .	38
5.6	全局最小割 . . . . .	40
5.7	支配树 . . . . .	41
5.8	最大团搜索 . . . . .	43
5.9	最小树形图 . . . . .	44
5.9.1	朱刘算法 . . . . .	44
5.9.2	可并堆优化 . . . . .	45
5.10	弦图 . . . . .	47
5.10.1	MCS 最大势算法。 . . . .	47
5.10.2	弦图判定 . . . . .	47
5.10.3	求弦图的团数与色数 . . . . .	47
5.10.4	求弦图的最大独立集和最小团覆盖 . . . . .	48

5.10.5 tricks	48
5.11 图计数相关	48
5.11.1 环计数	48
5.11.2 Prufer 序列	48
<b>6 多项式</b>	<b>50</b>
6.1 拉格朗日插值法	50
6.2 牛顿迭代	51
6.3 FFT	51
6.4 常用 NTT 模数及其原根	52
6.5 多项式模板	52
6.6 FWT	57
<b>7 计算几何</b>	<b>59</b>
7.1 计算几何模板	59
<b>8 杂项</b>	<b>66</b>
8.1 自定义哈希	66
8.1.1 splitmix 和仿函数	66
8.1.2 xorshift	67
8.1.3 手写哈希表	67
8.2 取模类	68
8.2.1 Barrett 约减	68
8.3 对拍脚本	69
8.4 VS Code 配置	69
8.4.1 User Tasks	69
8.4.2 设置	70
8.4.3 快捷键	71

# Chapter 1

## 字符串

### 1.1 最小表示法

---

```
1 // == Main ==
2 int i = 0, j = 1, k = 0;
3 while (k < n && i < n && j < n)
4     if (a[(i + k) % n] == a[(j + k) % n]) k++;
5     else {
6         if (a[(i + k) % n] > a[(j + k) % n]) i = i + k + 1;
7         else j = j + k + 1;
8         if (i == j) i++;
9         k = 0;
10    }
11 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,  $\text{pre}(s, i) \in \mathcal{B}(s) \iff |s| - i \in \mathcal{P}(s)$ 。

**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  $b$  是  $t$  的整周期, 则有  $b \in \mathcal{P}(s)$ 。

**周期引理:**

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

**定理 4:** 对于文本串  $s$  和模式串  $t$ , 若  $|t| \geq \frac{|s|}{2}$ , 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  $\text{pre}(s, p)$  划分成长度为  $|s| \bmod p$  的前缀和长度为  $p - |s| \bmod p$  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  $|t| \geq \frac{|s|}{2}$ , 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  $u$  是  $v$  的 Border。

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

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

## 1.2.2 KMP

```

1 // == Main ==
2 // n is |s|, m is |t|.
3 for (int i = 1, j = 0; i <= n; i++) {
4     while (j && t[j + 1] != s[i]) j = pi[j];
5     if (t[j + 1] == s[i])
6         if (++j == m) {

```

```

7         // ...
8         j = nxt[j];
9     }
10 }

```

---

## 1.3 Z 函数

```

1 // == Main ==
2 // n is |s|.
3 for (int i = 2, j = 0; i <= n; i++) {
4     if (i < j + z[j]) z[i] = min(z[i - j + 1], j + z[j] - i);
5     while (i + z[i] <= n && s[i + z[i]] == s[1 + z[i]]) z[i]++;
6     if (i + z[i] > j + z[j]) j = i;
7 }

```

---

## 1.4 Manacher

```

1 // == Main ==
2 // t is the original string, n is |t|.
3 string s = "^#";
4 for (char i : t) s.push_back(i), s.push_back('#');
5 s.push_back('@');
6 for (int i = 1, j = 0; i <= 2 * n + 1; i++) {
7     if (i <= j + p[j]) p[i] = min(p[2 * j - i], j + p[j] - i);
8     while (s[i - p[i] - 1] == s[i + p[i] + 1]) p[i]++;
9     if (i + p[i] > j + p[j]) j = i;
10 }

```

---

## 1.5 AC 自动机

```

1 // == Preparations ==
2 #include <queue>
3 // == Main ==
4 struct ACAM {
5     int tot, fail[200005], delta[200005][26];
6
7     void insert(string s, int id) {
8         int now = 0;
9         for (char c : s) {
10             int v = c - 'a';
11             if (!delta[now][v]) delta[now][v] = ++tot;

```

```

12         now = delta[now][v];
13     }
14     return;
15 }
16 void build() {
17     queue<int> q;
18     for (int c = 0; c < 26; c++)
19         if (delta[0][c]) q.push(delta[0][c]);
20     while (!q.empty()) {
21         int now = q.front();
22         q.pop();
23         for (int c = 0; c < 26; c++)
24             if (delta[now][c]) fail[delta[now][c]] = delta[fail[now]][c],
25                 ↪ q.push(delta[now][c]);
26             else delta[now][c] = delta[fail[now]][c];
27     }
28     return;
29 } ac;

```

---

## 1.6 回文自动机 PAM

```

1 // == Main ==
2 struct PAM {
3     int tot, delta[500005][26], len[500005], fail[500005], ans[500005];
4     string s;
5     int lst;
6
7     PAM() {tot = 1; len[0] = 0; len[1] = -1; fail[0] = fail[1] = 1;}
8     int getfail(int now, int i) {
9         while (s[i - len[now] - 1] != s[i]) now = fail[now];
10        return now;
11    }
12    void insert(int i) {
13        int now = getfail(lst, i);
14        if (!delta[now][s[i] - 'a']) {
15            len[++tot] = len[now] + 2;
16            fail[tot] = delta[getfail(fail[now], i)][s[i] - 'a'];
17            delta[now][s[i] - 'a'] = tot;
18            ans[tot] = ans[fail[tot]] + 1;
19        }
20        lst = delta[now][s[i] - 'a'];
21        return;
22    }
23 } p;

```

---



## 1.7 后缀自动机

### 1.7.1 普通 SAM

---

```

1 // == Main ==
2 struct SAM {
3     int tot, lst;
4     int len[2000005], siz[2000005], link[2000005];
5     int delta[2000005][26];
6
7     SAM() {link[0] = -1;}
8     void insert(char ch) {
9         int c = ch - 'a', now = ++tot;
10        len[now] = len[lst] + 1;
11        siz[now] = 1;
12        for (int p = lst; p != -1; p = link[p])
13            if (!delta[p][c]) delta[p][c] = tot;
14            else if (len[delta[p][c]] == len[p] + 1) {link[now] = delta[p][c];
15                ↪ break;}
16            else {
17                int q = delta[p][c], v = ++tot;
18                len[v] = len[p] + 1;
19                memcpy(delta[v], delta[q], sizeof(delta[v]));
20                link[v] = link[q], link[q] = v, link[now] = v;
21                for (int i = p; delta[i][c] == q; i = link[i]) delta[i][c] = v;
22                break;
23            }
24        lst = now;
25        return ;
26    }
27 } sam;

```

---

### 1.7.2 广义 SAM

注意自动机空间要开 Trie 的两倍。

---

```

1 // == Main ==
2 struct GSAM {
3     int tot;
4     int delta[2000005][26], link[2000005], len[2000005];
5     struct Trie {
6         int tot, trie[1000005][26], st[1000005];
7
8         void insert(string s) {
9             int now = 0;
10            for (char c : s) {

```

```

11         int id = c - 'a';
12         if (!trie[now][id]) trie[now][id] = ++tot;
13         now = trie[now][id];
14     }
15     return;
16 }
17 } tr;
18
19 GSAM() {link[0] = -1;}
20 int insert(int c, int lst) {
21     int now = ++tot;
22     len[now] = len[lst] + 1;
23     for (int p = lst; p != -1; p = link[p])
24         if (!delta[p][c]) delta[p][c] = now;
25         else if (len[delta[p][c]] == len[p] + 1) {link[now] = delta[p][c];
26             ↪ break;}
27         else {
28             int q = delta[p][c], v = ++tot;
29             len[v] = len[p] + 1;
30             memcpy(delta[v], delta[q], sizeof(delta[v]));
31             link[v] = link[q], link[q] = v, link[now] = v;
32             for (int i = p; i != -1 && delta[i][c] == q; i = link[i]) delta[i][c]
33                 ↪ = v;
34             break;
35         }
36     return now;
37 }
38 void build() {
39     queue<int> q;
40     tr.st[0] = 0;
41     q.push(0);
42     while (!q.empty()) {
43         int now = q.front();
44         q.pop();
45         for (int i = 0; i < 26; i++)
46             if (tr.trie[now][i])
47                 tr.st[tr.trie[now][i]] = insert(i, tr.st[now]),
48                 ↪ q.push(tr.trie[now][i]);
49     }
50     return;
51 }
52 } gsam;

```

---

## 1.8 后缀排序

---

```

1 // == Preparations ==
2 int sa[2000005], rk[2000005], b[1000005], cp[2000005];
3 // == Main ==
4 for (int i = 1; i <= n; i++) b[rk[i] = s[i]]++;
5 for (int i = 1; i < 128; i++) b[i] += b[i - 1];
6 for (int i = n; i >= 1; i--) sa[b[rk[i]]--] = i;
7 memcpy(cp, rk, sizeof(cp));
8 for (int i = 1, j = 0; i <= n; i++)
9     if (cp[sa[i]] == cp[sa[i - 1]]) rk[sa[i]] = j;
10    else rk[sa[i]] = ++j;
11 for (int w = 1; w < n; w <= 1) {
12     memcpy(cp, sa, sizeof(cp));
13     memset(b, 0, sizeof(b));
14     for (int i = 1; i <= n; i++) b[rk[cp[i] + w]]++;
15     for (int i = 1; i <= n; i++) b[i] += b[i - 1];
16     for (int i = n; i >= 1; i--) sa[b[rk[cp[i] + w]]--] = cp[i];
17     memcpy(cp, sa, sizeof(cp));
18     memset(b, 0, sizeof(b));
19     for (int i = 1; i <= n; i++) b[rk[cp[i]]]++;
20     for (int i = 1; i <= n; i++) b[i] += b[i - 1];
21     for (int i = n; i >= 1; i--) sa[b[rk[cp[i]]]--] = cp[i];
22     memcpy(cp, rk, sizeof(cp));
23     for (int i = 1, j = 0; i <= n; i++)
24         if (cp[sa[i]] == cp[sa[i - 1]] && cp[sa[i] + w] == cp[sa[i - 1] + w])
25             ↪ rk[sa[i]] = j;
26         else rk[sa[i]] = ++j;
27 }

```

---

# Chapter 2

## 数据结构

### 2.1 FHQ Treap

---

```
1 // == Preparations ==
2 #include <chrono>
3 #include <random>
4
5 mt19937 gen(chrono::system_clock::now().time_since_epoch().count());
6 // == Main ==
7 struct FHQ_Treap {
8     struct node {
9         int key, val, siz;
10        node *ls, *rs;
11
12        node() = default;
13        node(int _key): key(_key), val(gen()), siz(1), ls(nullptr), rs(nullptr) {}
14        void pushup() {
15            siz = 1;
16            if (ls) siz += ls->siz;
17            if (rs) siz += rs->siz;
18            return ;
19        }
20    };
21    node *root;
22
23    node *merge(node *u, node *v) {
24        if (!u) return v;
25        if (!v) return u;
26        if (u->val < v->val) {u->rs = merge(u->rs, v); u->pushup(); return u;}
27        else {v->ls = merge(u, v->ls); v->pushup(); return v;}
28    }
29    void split(node *now, int k, node *&u, node*&v) {
30        if (!now) {u = v = nullptr; return ;}
31        if (now->key < k) u = now, split(now->rs, k, u->rs, v);
```

```

32         else v = now, split(now->ls, k, u, v->ls);
33         now->pushup();
34         return ;
35     }
36     void insert(int k) {
37         node *u, *v;
38         split(root, k, u, v);
39         root = merge(u, merge(new node(k), v));
40         return ;
41     }
42     void erase(int k) {
43         node *u, *v, *w;
44         split(root, k, u, v), split(v, k + 1, v, w);
45         node *tmp = v;
46         v = merge(v->ls, v->rs);
47         delete tmp;
48         root = merge(u, merge(v, w));
49         return ;
50     }
51     int order_of_key(int k) {
52         node *u, *v;
53         split(root, k, u, v);
54         int ans = u ? u->siz + 1 : 1;
55         root = merge(u, v);
56         return ans;
57     }
58     int find_by_order(int k) {
59         node *now = root;
60         while (1) {
61             int lsiz = now->ls ? now->ls->siz : 0;
62             if (lsiz + 1 == k) return now->key;
63             else if (k <= lsiz) now = now->ls;
64             else k -= lsiz + 1, now = now->rs;
65         }
66     }
67     int find_prev(int k) {return find_by_order(order_of_key(k) - 1);}
68     int find_next(int k) {return find_by_order(order_of_key(k + 1));}
69 } tr;

```

---

## 2.2 K-D Tree

```

1 // == Main ==
2 template<const int Dim = 2>
3 struct KDTree {
4     using point = array<int, Dim>;
5     struct node {

```

```

6     point p, l, r;
7     int val, siz, sum;
8     node *ls, *rs;
9
10    node() = default;
11    node(point _p, int _val = 0):
12        p(_p), l(_p), r(_p), val(_val), siz(1), sum(_val), ls(nullptr),
13        ↪ rs(nullptr) {}
14    void pushup() {
15        l = r = p, siz = 1, sum = val;
16        for (int i = 0; i < Dim; i++) {
17            if (ls) l[i] = min(l[i], ls->l[i]), r[i] = max(r[i], ls->r[i]);
18            if (rs) l[i] = min(l[i], rs->l[i]), r[i] = max(r[i], rs->r[i]);
19        }
20        if (ls) siz += ls->siz, sum += ls->sum;
21        if (rs) siz += rs->siz, sum += rs->sum;
22        return ;
23    }
24    };
25    vector<node *> root;
26    using itor = typename vector<node*>::iterator;
27
28    node *build(itor l, itor r, int dim = 0) {
29        if (l == r) return nullptr;
30        int mid = (r - l) / 2;
31        nth_element(l, l + mid, r, [&dim](const node &x, const node &y) {return
32        ↪ x.p[dim] < y.p[dim];});
33        node *now = new node(*(l + mid));
34        now->ls = build(l, l + mid, (dim + 1) % Dim);
35        now->rs = build(l + mid + 1, r, (dim + 1) % Dim);
36        now->pushup();
37        return now;
38    }
39
40    void getnode(node *now, vector<node> &vec) {
41        if (!now) return ;
42        vec.push_back(*now);
43        getnode(now->ls, vec), getnode(now->rs, vec);
44        delete now;
45        return ;
46    }
47
48    void insert(point p, int val) {
49        vector<node> tmp({node(p, val)});
50        while (!root.empty() && root.back()->siz == (int)tmp.size())
51            getnode(root.back(), tmp), root.pop_back();
52        sort(tmp.begin(), tmp.end(), [](const node &x, const node &y) {return x.p <
53        ↪ y.p;});
54        vector<node> vec;
55        for (node i : tmp)
56            if (!vec.empty() && vec.back().p == i.p) vec.back().val += i.val;

```

```

52         else vec.push_back(i);
53     root.push_back(build(vec.begin(), vec.end()));
54     return ;
55 }
56 int query(point ll, point rr, node *now) {
57     if (!now) return 0;
58     int flag = 1;
59     for (int i = 0; i < Dim; i++)
60         if (now->r[i] < ll[i] || now->l[i] > rr[i]) return 0;
61         else flag &= ll[i] <= now->l[i] && now->r[i] <= rr[i];
62     if (flag) return now->sum;
63     flag = 1;
64     for (int i = 0; i < Dim; i++) flag &= ll[i] <= now->p[i] && now->p[i] <=
        rr[i];
65     return flag * now->val + query(ll, rr, now->ls) + query(ll, rr, now->rs);
66 }
67 int query(point ll, point rr) {
68     int ans = 0;
69     for (node *rt : root) ans += query(ll, rr, rt);
70     return ans;
71 }
72 ~KDTree() {
73     vector<node> tmp;
74     for (node *rt : root) getnode(rt, tmp);
75 }
76 };

```

---

## 2.3 Link Cut Tree

代码维护的是点权异或和。

```

1 // == Main ==
2 struct LinkCutTree {
3     int fa[100005], son[100005][2], siz[100005], swp[100005];
4     int val[100005], Xor[100005];
5
6     void pushup(int now) {
7         siz[now] = siz[son[now][0]] + siz[son[now][1]] + 1;
8         Xor[now] = Xor[son[now][0]] ^ val[now] ^ Xor[son[now][1]]; // 此处更新信息。
9         return;
10    }
11    void pushdown(int now) {
12        if(!swp[now]) return ;
13        swap(son[now][0], son[now][1]);
14        swp[son[now][0]] ^= 1, swp[son[now][1]] ^= 1;
15        swp[now] = 0;

```

```

16     // 此处将信息 pushdown
17     return;
18 }
19 int isRoot(int now) {return now != son[fa[now]][0] && now != son[fa[now]][1];}
20 int get(int now) {return now == son[fa[now]][1];}
21 void rotate(int x) {
22     int y = fa[x], z = fa[fa[x]], chk = get(x);
23     if (!isRoot(y)) son[z][get(y)] = x;
24     son[y][chk] = son[x][chk ^ 1], fa[son[x][chk ^ 1]] = y;
25     son[x][chk ^ 1] = y, fa[y] = x;
26     fa[x] = z;
27     pushup(y), pushup(x);
28     return;
29 }
30 void splay(int now) {
31     vector<int> stk;
32     stk.push_back(now);
33     for (int i = now; !isRoot(i); i = fa[i]) stk.push_back(fa[i]);
34     while (!stk.empty()) pushdown(stk.back()), stk.pop_back();
35     for (int f; f = fa[now], !isRoot(now); rotate(now))
36         if (!isRoot(f)) rotate(get(f) == get(now) ? f : now);
37     return;
38 }
39 void access(int now) { // 打通到根的链
40     for (int lst = 0; now; lst = now, now = fa[now]) splay(now), son[now][1] =
41         ↪ lst, pushup(now);
42     return;
43 }
44 void makeRoot(int now) {access(now); splay(now); swp[now] ^= 1; return;} // 设置
45 ↪ 根
46 void link(int u, int v) {makeRoot(u); fa[u] = v; return;} // 连接
47 void cut(int u, int v) {makeRoot(u); access(v); splay(v); son[v][0] = fa[u] = 0;
48 ↪ return;} // 切割
49 int find(int now) { // 找根
50     access(now), splay(now);
51     pushdown(now);
52     while (son[now][0]) now = son[now][0], pushdown(now);
53     splay(now);
54     return now;
55 }
56 void split(int u, int v) {makeRoot(u); access(v); splay(u); return;} // 剖出 u ~
57 ↪ v 的链
58 void update(int u, int _val) {split(u, u); val[u] = Xor[u] = _val; return;} //
59 ↪ 修改操作, split 后做就行了, 此处为单点修改。
60 int query(int u, int v) {split(u, v); return Xor[u];} // 查询操作, split 后做就行
61 ↪ 了。
62 int isConnected(int u, int v) {return find(u) == find(v);} // 查询两个点是否连通。
63 };

```



# 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, 11, 13, 17, 19, 23, 29, 31, 37};
3
4 long long power(long long a, long long b, long long mod) {
5     long long ans = 1;
6     while (b) {
7         if (b & 1) ans = (__int128)ans * a % mod;
8         a = (__int128)a * a % mod;
9         b >>= 1;
10    }
11    return ans % mod;
12 }
13 // == Main ==
14 inline int Miller_Rabin(long long n) {
15     if (n == 1) return 0;
16     if (n == 2) return 1;
17     if (n % 2 == 0) return 0;
18     long long u = n - 1, t = 0;
19     while (u % 2 == 0) u /= 2, t++;
20     for (int i = 0; i < 12; i++) {
21         if (prime[i] % n == 0) continue;
22         long long x = power(prime[i] % n, u, n);
23         if (x == 1) continue;
24         int flag = 0;
25         for (int j = 1; j <= t; j++) {
26             if (x == n - 1) {flag = 1; break;}
27             x = (__int128)x * x % n;
28         }
29         if (!flag) return 0;
```

```

30     }
31     return 1;
32 }

```

---

### 3.1.2 Pollard Rho

---

```

1 // == Preparations ==
2 #include <chrono>
3 #include <random>
4
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) {
11     long long s = 0, t = 0, c = gen() % (n - 1) + 1;
12     for (int goal = 1; ; goal <= 1, s = t) {
13         long long val = 1;
14         for (int step = 1; step <= goal; step++) {
15             t = ((__int128)t * t + c) % n;
16             val = ((__int128)val * abs(t - s) % n;
17             if (!val) return n;
18             if (step % 127 == 0) {
19                 long long d = __gcd(val, n);
20                 if (d > 1) return d;
21             }
22         }
23         long long d = __gcd(val, n);
24         if (d > 1) return d;
25     }
26 }
27 void factor(long long n) {
28     if (n < ans) return ;
29     if (n == 1 || Miller_Rabin(n)) {
30         // n = 1 或 n 是一个质因子。
31         // ...
32     }
33     long long p;
34     do p = Pollard_Rho(n);
35     while (p == n);
36     while (n % p == 0) n /= p;
37     factor(n), factor(p);
38     return ;
39 }

```

---

## 3.2 常用数论算法

### 3.2.1 exgcd

求出来的解满足  $|x| \leq b, |y| \leq a$ 。

---

```

1 // == Main ==
2 int exgcd(int a, int b, int &x, int &y) {
3     if (b == 0) {x = 1; y = 0; return a;}
4     int m = exgcd(b, a % b, y, x);
5     y -= a / b * x;
6     return m;
7 }

```

---

### 3.2.2 CRT

没用。

---

```

1 // == 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;

```

```

9      long long g = exgcd(a, b, x, y);
10     if (c % g != 0) return -1;
11     b /= g;
12     x = (__int128)x * (c / g) % b;
13     ans += x * mod;
14     mod *= b;
15     ans = (ans % mod + mod) % mod;
16 }
17 return ans;
18 }

```

---

### 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) {
7     int x, y;
8     exgcd(n, p, x, y);
9     return (x % p + p) % p;
10 }
11 int fac(long long n, int p, int pk) {
12     if (n == 0) return 1;
13     int res = 1;
14     for (int i = 1; i < pk; i++)
15         if (i % p != 0) res = (long long)res * i % pk;
16     res = power(res, n / pk, pk);
17     for (int i = 1; i <= n % pk; i++)
18         if (i % p != 0) res = (long long)res * i % pk;
19     return (long long)res * fac(n / p, p, pk) % pk;
20 }
21 int C(long long n, long long m, int p, int pk) {
22     long long x = n, y = m, z = n - m;
23     int res = (long long)fac(x, p, pk) * inv(fac(y, p, pk), pk) % pk * inv(fac(z, p,
24         ↪ pk), pk) % pk;
25     long long e = 0;
26     while (x) e += x / p, x /= p;
27     while (y) e -= y / p, y /= p;
28     while (z) e -= z / p, z /= p;
29     return (long long)res * power(p, e, pk) % pk;
30 }
31 int exLucas(long long n, long long m, int p) {
32     vector<pair<int, int>> a;
33     for (int i = 2; i * i <= p; i++)
34         if (p % i == 0) {

```

```

34         int pk = 1;
35         while (p % i == 0) pk *= i, p /= i;
36         a.emplace_back(C(n, m, i, pk), pk);
37     }
38     if (p != 1) a.emplace_back(C(n, m, p, p), p);
39     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  $y$  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  $\text{euclid}(a, b, c, n, u, r)$ 。

其中  $a, b \geq 0, n, c > 0$ 。

做法:

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

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

```

1 // == Preparations ==
2 struct Node {
3     // ...
4
5     Node operator*(const Node &x) const {
6         // ...
7     }
8 };
9 // == Main ==
10 Node power(Node a, long long b) {
11     Node ans = Node(/* 幺元 */);
12     while (b) {
13         if (b & 1) ans = ans * a;
14         a = a * a;

```

```

15         b >>= 1;
16     }
17     return ans;
18 }
19 Node Euclid(int a, int b, int c, long long n, Node r, Node u) {
20     long long m = (a * n + b) / c;
21     if (!m) return power(r, n);
22     if (a >= c || b >= c)
23         return power(u, b / c) * Euclid(a % c, b % c, c, n, power(u, a / c) * r, u);
24     return power(r, (c - b - 1) / a) * u *
25         Euclid(c, (c - b - 1) % a, a, m - 1, u, r) * power(r, n - (c * m - b - 1) /
26             ↪ a);
27 }

```

## 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  $0 \leq k < \varphi(m)$  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  $M$  且  $x = AM - B$ ，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  $a \perp p, 2 \leq b, n < p < 2^{31}$ ，求得的是模意义下  $\log_a b$  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);

```

```

12     sz = sqrt(phi / m) + 1;
13     t = ((ll)phi + sz - 1) / sz;
14     int as = Qpow(a , sz , p) , aa = 1;
15     for(int i = 1 ; i <= t ; i++)
16     {
17         aa = (ll)aa * as % p;
18         if(!mp[aa])mp[aa] = i;
19     }
20 }
21 int BSGS(int b)
22 {
23     int r = b , ans = p;
24     for(int k = 0 ; k <= sz ; k++)
25     {
26         if(mp.find(r) != mp.end())
27             ans = min((ll)ans , (ll)mp[r] * sz - k);
28         r = (ll)r * a % p;
29     }
30     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  $x \leq k$  的情况。

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

---

```

1 // == Preparations ==
2 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 {
11     mp.clear() , low.clear();
12     a %= p , mod = p , d = 1 , k = 0;
13     int ad = 1 , ak = 1;
14     for(int g = __gcd(a , p) ; g != 1 ; g = __gcd(a , p))
15     {
16         ak = (ll)ak * a % mod , k++;

```

```

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

**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  $k \in \mathbf{N}$ ,  $m$  为正整数,  $a \in \mathbf{Z}$ ,  $(a, m) = 1$ , 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  $g^i \bmod m, 0 < i < m$  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;

```

```

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

$$x^k \equiv a \pmod{m} \quad (1)$$

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  $k \geq 2$  , 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  $d \mid \text{ind}_g a$  , 即:  $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$

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

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

由同余的性质, 我们知道  $y$  有整数解当且仅当  $d = (k, \varphi(m)) \mid \text{ind}_g a$  , 进而

$$\begin{aligned}
 a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m} &\iff g^{\frac{\varphi(m)}{d} \text{ind}_g a} \equiv 1 \pmod{m} \\
 &\iff \varphi(m) \mid \frac{\varphi(m)}{d} \text{ind}_g a \\
 &\iff \varphi(m)d \mid \varphi(m) \text{ind}_g a \\
 &\iff d \mid \text{ind}_g a
 \end{aligned}$$

**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

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

### 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 {
7     int a , b;
8     Complex(ll aa = 0 , ll bb = 0):a(aa % mod) , b(bb % mod){}
9 };
10 typedef Complex cp;
11 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 {
15     return cp((ll)x.a * y.a + (ll)w2 * x.b % mod * y.b ,
16               (ll)x.b * y.a + (ll)y.b * x.a);
17 }
18 cp Qpow(cp x , int p)
19 {
20     cp res = 1;
21     while(p)
22     {
23         if(p & 1)res = res * x;
24         x = x * x;

```

```

25     p >>= 1;
26 }
27 return res;
28 }
29 // == Main ==
30 int Legendre(int a){return Qpow(a , (mod - 1) / 2).a;}
31 pair<int , int> Cipolla(int a)
32 {
33     if(a % mod == 0)return {0 , -1};
34     if(Legendre(a) == mod - 1)return {-1 , -1};
35     int res = 0;
36     while(1)
37     {
38         int r = rnd() % mod;
39         w2 = ((1ll)r * r - a) % mod;
40         if(w2 < 0)w2 += mod;
41         if(w2 == 0)
42         {
43             res = r;
44             break ;
45         }
46         if(Legendre(w2) == mod - 1)
47         {
48             res = Qpow(cp(r , 1) , (mod + 1) / 2).a;
49             break ;
50         }
51     }
52     if(res * 2 >= mod)res = mod - res;
53     return {res , mod - res};
54 }

```

---

### 3.6.3 模素数 $N$ 次剩余

我们令  $x = g^c$  ,  $g$  是  $p$  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  $sp_i = \sum_{j=1}^i p_j$ ,  $D$  为最大的  $i$  满足  $p_i^2 \leq n$ , 容易得出转移:

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

然后暴力递归求出  $s$  就行了, 不需要记忆化。

### 3.7.2 求素数个数

---

```

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)
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(){
10     //预处理根号以内质数
11     rep(i,2,lim){
12         if (!vis[i]) prime[++prime[0]]=i;
13         for (int j=1;j<=prime[0] && i*prime[j]<=lim;++j){
14             vis[i*prime[j]]=1;
15             if (i%prime[j]==0) break;
16         }
17     }
18 }
19 inline void solve(){

```

```

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

```

---

### 3.7.3 完整模板

```

1 // == Preparations ==
2 #define int long long
3 #define rep(i,j,k) for(int i=j;i<=k;++i)
4 #define per(i,j,k) for(int i=j;i>=k;--i)
5 #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
9 //发现  $f(p^k)=p^{\{2k\}}-p^k$ 
10 int const mod=1e9+7;
11 int n;
12 inline int f(int op,int x){
13     x%=mod;
14     if (!op) return x;
15     return x*x%mod;
16 }
17 inline int F(int x){
18     x%=mod;
19     return x*(x-1)%mod;
20 }
21 inline int smf(int op,int x){
22     x%=mod;
23     if (!op) return (x*(x+1)/2)%mod;
24     return x*(x+1)%mod*(2*x%mod+1)%mod*166666668%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(){
30     //预处理根号以内质数
31     rep(i,2,lim){
32         if (!vis[i]) prime[++prime[0]]=i;

```

```

33     for (int j=1;j<=prime[0] && i*prime[j]<=lim;++j){
34         vis[i*prime[j]]=1;
35         if (i%prime[j]==0) break;
36     }
37 }
38 rep(i,1,prime[0]){
39     sp1[i]=sp1[i-1],add(sp1[i],f(0,prime[i]));
40     sp2[i]=sp2[i-1],add(sp2[i],f(1,prime[i]));
41 }
42 }
43 inline int S(int x,int y){
44     if (prime[y]>=x) return 0;
45     int ans=((g2[id(x)]+mod-g1[id(x)])%mod+mod-(sp2[y]-sp1[y]+mod)%mod)%mod;
46     for (int i=y+1;i<=prime[0] && prime[i]*prime[i]<=x;++i)
47         for (int e=1,gg=prime[i];gg<=x;++e,gg*=prime[i])
48             add(ans,F(gg)*(S(x/gg,i)+(e>1))%mod);
49     return ans;
50 }
51 inline void solve(){
52     cin>>n,lim=sqrtl(n),init();
53     for (int l=1,r;l<=n;l=r+1){
54         r=n/(n/l),w[++m]=n/l;
55         g1[m]=(smf(0,w[m])+mod-1)%mod;
56         g2[m]=(smf(1,w[m])+mod-1)%mod;
57         if (w[m]<=lim) id1[w[m]]=m;
58         else id2[n/w[m]]=m;
59         //预处理 g 数组第一维有可能的取值
60     }
61     rep(i,1,prime[0])
62         for (int j=1;j<=m && prime[i]*prime[i]<=w[j];++j)
63             add(g1[j],mod-f(0,prime[i])*(g1[id(w[j]/prime[i])]+mod-sp1[i-1])%mod),
64             add(g2[j],mod-f(1,prime[i])*(g2[id(w[j]/prime[i])]+mod-sp2[i-1])%mod);
65     cout<<(S(n,0)+1)%mod<<"\n";
66 }

```

---

# Chapter 4

## 线性代数

### 4.1 行列式求值

---

```
1 // == Preparations ==
2 const int N = 605;
3 // == Main ==
4 void Swap(int i , int j)
5 {
6     if(i == j) return ;
7     for(int k = 1 ; k <= n ; k++)
8         swap(a[i][k] , a[j][k]);
9     f = -f;
10 }
11 int Det(int n , int mod , ll a[N][N])
12 {
13     int m = 0;
14     for(int i = 1 ; i <= n ; i++)
15     {
16         m++;
17         for(int j = m ; j <= n ; j++)
18             if(a[j][i]){Swap(m , j); break ;};
19         if(!a[m][i]) return 0;
20         for(int j = m + 1 ; j <= n ; j++)
21         {
22             while(a[j][i] && a[m][i])
23             {
24                 ll r = a[j][i] / a[m][i] % mod;
25                 for(int k = 1 ; k <= n ; k++)
26                     a[j][k] = (a[j][k] - (ll)r * a[m][k]) % mod;
27                 Swap(m , j);
28             }
29             if(!a[m][i]) Swap(m , j);
30         }
31     }
```



```
32     ll ans = 1;
33     for(int i = 1 ; i <= n ; i++)
34         ans *= a[i][i];
35     return (ans * f % mod + mod) % mod;
36 }
```

---

# Chapter 5

## 图论

### 5.1 Tarjan

#### 5.1.1 强连通分量

---

```
1 // == Main ==
2 void Tarjan(int now) {
3     dfn[now] = low[now] = ++Index;
4     s.push(now);
5     for (int i = g.hd[now]; i; i = g.nxt[i])
6         if (!dfn[g.to[i]]) {
7             Tarjan(g.to[i]);
8             low[now] = min(low[now], low[g.to[i]]);
9         } else if (!scc[g.to[i]]) low[now] = min(low[now], dfn[g.to[i]]);
10    if (low[now] == dfn[now]) {
11        scc_cnt++;
12        for (int x = 0; x != now; s.pop()) {
13            x = s.top();
14            scc[x] = scc_cnt;
15        }
16    }
17    return ;
18 }
```

---

#### 5.1.2 割边与边双

割边:

---

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

```

6         Tarjan(g.to[i], now);
7         low[now] = min(low[now], low[g.to[i]]);
8         if (low[g.to[i]] > dfn[now])
9             printf("A Bridge of the Input Garph is (%d, %d)\n", now, g.to[i]);
10    } else if (g.to[i] != fa) low[now] = min(low[now], dfn[g.to[i]]);
11    return ;
12 }

```

---

边双:

```

1 // == Main ==
2 void Tarjan(int now, int fa) {
3     dfn[now] = low[now] = ++Index;
4     s.push(now);
5     for (int i = g.hd[now]; i; i = g.nxt[i])
6         if (!dfn[g.to[i]]) {
7             Tarjan(g.to[i], now);
8             low[now] = min(low[now], low[g.to[i]]);
9         } else if (g.to[i] != fa) low[now] = min(low[now], dfn[g.to[i]]);
10    if (low[now] == dfn[now]) {
11        bcc_cnt++;
12        for (int x = 0; x != now; s.pop()) {
13            x = s.top();
14            bcc[x] = bcc_cnt;
15        }
16    }
17    return ;
18 }

```

---

### 5.1.3 割点与点双

割点:

```

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

```

```

14     return ;
15 }

```

---

点双:

```

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

```

---

## 5.2 欧拉路径

```

1 // == Preparations ==
2 #include <vector>
3
4 vector<int> g[100005], ans;
5 // == Main ==
6 void dfs(int now) {
7     while (!g[now].empty()) {
8         int to = g[now].back();
9         g[now].pop_back();
10        dfs(to);
11    }
12    ans.push_back(now);
13    return ;
14 }

```

---

## 5.3 二分图匹配

### 5.3.1 最大匹配

---

```

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

```

---

### 5.3.2 最大权匹配

---

```

1 // == Preparations ==
2 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++) {
8     w[i] = ~0x3f3f3f3f3f3f3f3f;
9     for (int j = n + 1; j <= n + n; j++) w[i] = max(w[i], (long long)g[i][j]);
10 }
11 for (int i = 1; i <= n; i++) {
12     memset(vis, 0, sizeof(vis));
13     memset(slack, 0x3f, sizeof(slack));
14     memset(pre, 0, sizeof(pre));
15     int now = i, ri = 0;
16     while (1) {
17         int id = 0;
18         long long delta = 0x3f3f3f3f3f3f3f3f;
19         for (int j = n + 1; j <= n + n; j++)

```

---

```

20         if (!vis[j]) {
21             long long val = w[now] + w[j] - g[now][j];
22             if (val < slack[j]) slack[j] = val, pre[j] = ri;
23             if (slack[j] < delta) delta = slack[j], id = j;
24         }
25     w[i] -= delta;
26     for (int j = n + 1; j <= n + n; j++)
27         if (vis[j]) w[j] += delta, w[mat[j]] -= delta;
28         else slack[j] -= delta;
29     vis[ri = id] = 1;
30     if (mat[ri]) now = mat[ri];
31     else break;
32 }
33 while (ri) {
34     mat[ri] = mat[pre[ri]];
35     if (!pre[ri]) {mat[ri] = i; break;}
36     ri = pre[ri];
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 {
5     int s, t;
6     struct graph {
7         int tot, hd[205];
8         int nxt[10005], to[10005], dt[10005];
9         graph() {tot = 1;}
10        void add(int u, int v, int w) {
11            nxt[++tot] = hd[u];
12            hd[u] = tot;
13            to[tot] = v;
14            dt[tot] = w;
15            return ;
16        }
17    } g;

```

```

18     int cur[205], dis[205];
19
20     void add_edge(int u, int v, int f) {g.add(u, v, f), g.add(v, u, 0); return;}
21     int bfs() {
22         memset(dis, 0, sizeof(dis));
23         queue<int>q;
24         q.push(s);
25         dis[s] = 1;
26         while (!q.empty()) {
27             int now = q.front();
28             q.pop();
29             cur[now] = g.hd[now];
30             for (int i = g.hd[now]; i; i = g.nxt[i])
31                 if (g.dt[i] && !dis[g.to[i]]) dis[g.to[i]] = dis[now] + 1,
32                     ↪ q.push(g.to[i]);
33         }
34         return dis[t];
35     }
36     long long dinic(int now, long long flow) {
37         if (now == t) return flow;
38         long long used = 0;
39         for (int i = cur[now]; i && used < flow; i = g.nxt[i])
40             if (g.dt[i] && dis[g.to[i]] == dis[now] + 1) {
41                 long long k = dinic(g.to[i], min(flow - used, (long long)g.dt[i]));
42                 g.dt[i] -= k, g.dt[i ^ 1] += k;
43                 used += k;
44                 cur[now] = i;
45             }
46         if (used == 0) dis[now] = 0;
47         return used;
48     }
49     long long solve() {
50         long long ans = 0;
51         while (bfs()) ans += dinic(s, 0x3f3f3f3f3f3f3f3f);
52         return ans;
53 } F;

```

---

## 5.4.2 费用流

原始对偶：

---

```

1 // == Preparations ==
2 #include <queue>
3 // == Main ==
4 struct PrimalDual {
5     int n, s, t;

```

```

6  struct graph {
7      int tot, hd[805];
8      int nxt[30005], to[30005], flw[30005], cst[30005];
9
10     graph() {tot = 1;}
11     void add(int u, int v, int f, int c) {
12         nxt[++tot] = hd[u];
13         hd[u] = tot;
14         to[tot] = v;
15         flw[tot] = f;
16         cst[tot] = c;
17         return ;
18     }
19 } g;
20 int h[805], dis[805], f[805], pre[805];
21 struct node {
22     int id, val;
23
24     node() = default;
25     node(int _id, int _val): id(_id), val(_val) {}
26     bool operator<(const node &x) const {return val > x.val;}
27 };
28
29 void add_edge(int u, int v, int f, int c) {g.add(u, v, f, c), g.add(v, u, 0, -c);
    ↪ return;}
30 void spfa() {
31     queue<int> q;
32     memset(h, 0x3f, sizeof(h));
33     h[s] = 0;
34     q.push(s);
35     while (!q.empty()) {
36         int now = q.front();
37         q.pop();
38         f[now] = 0;
39         for (int i = g.hd[now]; i; i = g.nxt[i])
40             if (g.flw[i] && h[g.to[i]] > h[now] + g.cst[i]) {
41                 h[g.to[i]] = h[now] + g.cst[i];
42                 if (!f[g.to[i]]) q.push(g.to[i]), f[g.to[i]] = 1;
43             }
44     }
45     return ;
46 }
47 int dijkstra() {
48     priority_queue<node> q;
49     memset(dis, 0x3f, sizeof(dis));
50     memset(pre, 0, sizeof(pre));
51     q.emplace(s, dis[s] = 0);
52     while (!q.empty()) {
53         int now = q.top().id, tmp = q.top().val;

```



```

54     q.pop();
55     if (dis[now] != tmp) continue;
56     for (int i = g.hd[now]; i; i = g.nxt[i])
57         if (g.flw[i] && dis[g.to[i]] > dis[now] + g.cst[i] + h[now] -
58             ↪ h[g.to[i]]) {
59             q.emplace(g.to[i], dis[g.to[i]] = dis[now] + g.cst[i] + h[now] -
60                 ↪ h[g.to[i]]);
61             pre[g.to[i]] = i ^ 1;
62         }
63     }
64     return pre[t];
65 }
66 pair<int, int> solve() {
67     int flow = 0, cost = 0;
68     spfa();
69     while (dijkstra()) {
70         for (int i = 1; i <= n; i++)
71             if (dis[i] < 0x3f3f3f3f) h[i] += dis[i];
72         int mnflow = 0x3f3f3f3f;
73         for (int i = t; i != s; i = g.to[pre[i]]) mnflow = min(mnflow,
74             ↪ g.flw[pre[i] ^ 1]);
75         for (int i = t; i != s; i = g.to[pre[i]]) g.flw[pre[i] ^ 1] -= mnflow,
76             ↪ g.flw[pre[i]] += mnflow;
77         flow += mnflow;
78         cost += mnflow * h[t];
79     }
80     return {flow, cost};
81 }
82 } 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  $s$  向  $u$  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 ==
2 int ontree[200005];
3 struct graph {
4     int tot, hd[5005];
5     int nxt[200005], to[200005];
6     long long dt[200005];
7
8     void add(int u, int v, long long w) {
9         nxt[++tot] = hd[u];
10        hd[u] = tot;
11        to[tot] = v;
12        dt[tot] = w;
13        return ;
14    }

```

```

15 } g;
16 long long dis[5005];
17 struct node {
18     int id;
19     long long val;
20
21     node() = default;
22     node(int _id, long long _val): id(_id), val(_val) {}
23     bool operator<(const node &x) const {return val > x.val;}
24 };
25 priority_queue<node> q;
26 int vis[5005];
27
28 // 以下左偏树
29 struct HeapNode {
30     long long val;
31     int to, dist;
32     HeapNode *ls, *rs;
33
34     HeapNode() = default;
35     HeapNode(long long _val, int _to): val(_val), to(_to), dist(1), ls(nullptr),
        ↪ rs(nullptr) {}
36 };
37 struct Heap {
38     HeapNode *root[5005];
39
40     HeapNode *merge(HeapNode *u, HeapNode *v) {
41         if (!u) return v;
42         if (!v) return u;
43         if (u->val > v->val) swap(u, v);
44         HeapNode *p = new HeapNode(*u);
45         p->rs = merge(u->rs, v);
46         if (!p->ls || p->ls->dist < p->rs->dist) swap(p->ls, p->rs);
47         if (p->rs) p->dist = p->rs->dist + 1;
48         else p->dist = 1;
49         return p;
50     }
51 } h;
52
53 struct Node {
54     HeapNode *id;
55     long long val;
56
57     Node() = default;
58     Node(HeapNode *_id, long long _val): id(_id), val(_val) {}
59     bool operator<(const Node &x) const {return val > x.val;}
60 };
61 priority_queue<Node> Q;
62 // == Main ==

```

```

63 void dfs(int now) {
64     vis[now] = 1;
65     for (int i = g.hd[now]; i; i = g.nxt[i])
66         if (!vis[g.to[i]] && dis[g.to[i]] == dis[now] + g.dt[i]) ontree[i] = 1,
            ↪ dfs(g.to[i]);
67     return ;
68 }
69 void dfs2(int now) {
70     for (int i = g.hd[now]; i; i = g.nxt[i])
71         if (ontree[i]) h.root[g.to[i]] = h.merge(h.root[g.to[i]], h.root[now]),
            ↪ dfs2(g.to[i]);
72     return;
73 }
74
75 memset(dis, 0x3f, sizeof(dis));
76 q.emplace(n, dis[n] = 0);
77 while (!q.empty()) {
78     int now = q.top().id;
79     long long tmp = q.top().val;
80     q.pop();
81     if (tmp != dis[now]) continue;
82     for (int i = g.hd[now]; i; i = g.nxt[i])
83         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++)
87     for (int j = g.hd[i]; j; j = g.nxt[j])
88         if (!ontree[j] && g.to[j] != n)
89             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);
92 while (!Q.empty()) { // 每次取出来一条路径
93     HeapNode *now = Q.top().id;
94     long long d = Q.top().val;
95     Q.pop();
96     if (now->ls) Q.emplace(now->ls, d - now->val + now->ls->val);
97     if (now->rs) Q.emplace(now->rs, d - now->val + now->rs->val);
98     HeapNode *tmp = h.root[now->to];
99     if (tmp) Q.emplace(tmp, d + tmp->val);
100 }

```

---

## 5.6 全局最小割

时间复杂度为  $O(|V|^3)$ 。

---

```

1 // == Preparations ==
2 int g[605][605], vis1[605], vis2[605];
3 long long w[605];
4 // == Main ==
5 long long Stoer_Wagner() {
6     long long ans = 0x3f3f3f3f3f3f3f3f;
7     for (int i = 1; i < n; i++) {
8         int s = 0, t = 0;
9         memset(vis2, 0, sizeof(vis2));
10        memset(w, 0, sizeof(w));
11        for (int j = 1; j <= n - i + 1; j++) {
12            int now = 0;
13            for (int k = 1; k <= n; k++)
14                if (!vis1[k] && !vis2[k] && w[k] >= w[now]) now = k;
15            s = t, t = now;
16            vis2[now] = 1;
17            for (int k = 1; k <= n; k++) w[k] += g[k][now];
18        }
19        ans = min(ans, w[t]);
20        vis1[t] = 1;
21        for (int j = 1; j <= n; j++)
22            if (j != s) g[s][j] += g[t][j], g[j][s] += g[j][t];
23    }
24    return ans;
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。

---

```

1 // == Preparations ==
2 #include <vector>
3
4 struct graph {
5     int tot, hd[200005];
6     int nxt[300005], to[300005];
7
8     void add(int u, int v) {
9         nxt[++tot] = hd[u];
10        hd[u] = tot;
11        to[tot] = v;
12        return ;
13    }
14 } g, fg;

```

```

15 int timer, fa[200005], dfn[200005], id[200005];
16 int sdom[200005], idom[200005];
17 struct dsu {
18     int fa[200005], mn[200005];
19
20     dsu() {for (int i = 1; i < 200005; i++) fa[i] = mn[i] = i;}
21     int find(int x) {
22         if (x == fa[x]) return x;
23         int tmp = find(fa[x]);
24         if (dfn[sdom[mn[fa[x]]]] < dfn[sdom[mn[x]]]) mn[x] = mn[fa[x]];
25         return fa[x] = tmp;
26     }
27 } d;
28 vector<int> vec[200005];
29 int siz[200005];
30 // == Main ==
31 void dfs(int now) {
32     id[dfn[now] = ++timer] = now;
33     for (int i = g.hd[now]; i; i = g.nxt[i])
34         if (!dfn[g.to[i]]) fa[g.to[i]] = now, dfs(g.to[i]);
35     return ;
36 }
37 void solve() {
38     dfs(1);
39     for (int i = 1; i <= n; i++) sdom[i] = i;
40     for (int i = timer; i >= 1; i--) {
41         int u = id[i];
42         for (int v : vec[u]) {
43             d.find(v);
44             if (sdom[d.mn[v]] == u) idom[v] = u;
45             else idom[v] = d.mn[v];
46         }
47         if (i == 1) continue;
48         for (int j = fg.hd[u]; j; j = fg.nxt[j]) {
49             if (!dfn[fg.to[j]]) continue;
50             if (dfn[fg.to[j]] < dfn[sdom[u]]) sdom[u] = fg.to[j];
51             else if (dfn[fg.to[j]] > dfn[u]) {
52                 d.find(fg.to[j]);
53                 if (dfn[sdom[d.mn[fg.to[j]]]] < dfn[sdom[u]]) sdom[u] =
54                     ↪ sdom[d.mn[fg.to[j]]];
55             }
56             vec[sdom[u]].push_back(u);
57             d.fa[u] = fa[u];
58         }
59     }
60     for (int i = 2; i <= timer; i++)
61         if (idom[id[i]] != sdom[id[i]]) idom[id[i]] = idom[idom[id[i]]];
62     return ;

```

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;
5 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 {
9     if(!P)
10     {
11         if(!X) ans = max(ans , popc(R)); //now R is the maximal clique
12         return ;
13     }
14     ll v = __lg(P | X);
15     for(ll s = P ^ (P & g[v]) ; s ; s -= s & -s)
16     {
17         ll u = __lg(s & -s);
18         Dfs(R | (1ll << u) , P & g[u] , X & g[u]);
19         P ^= 1ll << u , X |= 1ll << u;
20     }
21 }
22 void BronKerbosch()
23 {
24     for(int i = 0 ; i < n ; i++) d[i] = g[i];
25     for(int i = 0 ; i < n ; i++)
26     {
27         int &k = a[i]; k = -1;
28         for(int j = 0 ; j < n ; j++)
29             if(d[j] != -1 && (k == -1 || popc(d[j]) <= popc(d[k])))
30                 k = j;
31         d[k] = -1;
32         for(int j = 0 ; j < n ; j++)
33             if(d[j] >= 0 && (d[j] >> k) & 1) d[j] ^= 1ll << k;
34     }
35     ll P = (1ll << n) - 1 , X = 0;
36     for(int i = 0 ; i < n ; i++)
37     {

```

```

38     int u = a[i];
39     Dfs(1ll << u , P & g[u] , X & g[u]);
40     P ^= 1ll << u , X |= 1ll << u;
41 }
42 }

```

---

## 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 {
3     while(1)
4     {
5         fill(mn + 1 , mn + n + 1 , 1e9);
6         fill(id + 1 , id + n + 1 , 0);
7         fill(top + 1 , top + n + 1 , 0);
8         for(int i = 1 ; i <= m ; i++)
9         {
10             auto [u , v , w] = e[i];
11             if(w < mn[v])mn[v] = w , fa[v] = u;
12         }
13         for(int i = 1 ; i <= n ; i++)
14         {
15             if(i == rt)continue ;
16             if(mn[i] != 1e9)ans += mn[i];
17             else return 0;
18         }
19         int cnt = 0 , tot = 0;
20         for(int i = 1 ; i <= n ; i++)
21         {
22             if(id[i] || i == rt)continue ;
23             int u = i;
24             for(; u != rt && !top[u] ; u = fa[u])top[u] = i;
25             if(top[u] == i)
26             {
27                 id[u] = ++cnt;
28                 for(int v = fa[u] ; v != u ; v = fa[v])
29                     id[v] = cnt;
30             }
31         }
32         if(!cnt)return 1;

```



```

33     for(int i = 1 ; i <= n ; i++)
34         if(!id[i])id[i] = ++cnt;
35     for(int i = 1 ; i <= m ; i++)
36     {
37         auto [u , v , w] = e[i];
38         if(id[u] == id[v])continue ;
39         e[++tot] = {id[u] , id[v] , w - mn[v]};
40     }
41     n = cnt , m = tot , rt = id[rt];
42 }
43 }

```

## 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  $w(\text{in}(u))$ ，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  $(i, i \bmod n + 1, +\infty)$ 。

**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  $\text{in}$ ，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  $\text{in}(u)$ 。
3. 从  $v = pre_u$  开始依次访问环上的点，跳  $v = pre_v$ ，所有  $\text{in}(v)$  就是环上的边，答案加上  $w(\text{in}(v))$ 。  
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 **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 {
9     int fa[N];
10    void init(int n){iota(fa + 1 , fa + n + 1 , 1);}
11    int find(int x){return x == fa[x] ? x : fa[x] = find(fa[x]);}
12    int& operator [](int x){return fa[find(x)];}
13 }col , id;
14 // == Main ==
15 bool Work(int u)
16 {
17     while(pq[u] && (in[u] = pq[u].top().se , pre(u) == u))
18         pq[u].pop();
19     if(!pq[u])return 0;
20     auto [w , i] = pq[u].top(); int v = pre(u);
21     in[u] = i , pq[u].tag -= w , pq[u].pop();
22     if(col[u] != col[v])
23     {
24         col[u] = col[v];
25         return 1;
26     }
27     pq[++num].merge(pq[u]) , col[u] = col[num];
28     for(int x = v ; x != u ; pre[x] = pre(x) , x = pre[x])
29         f[x] = id[x] = num , pq[num].merge(pq[x]);
30     f[u] = id[u] = num , pre[u] = v;
31     return Work(num);
32 }
33 ll Expand(ll u , ll rt)
34 {
35     ll ans = 0;
36     for(; u != rt ; u = f[u])
37     {
38         for(int v = pre[u] ; v != u ; v = pre[v])
39         {
40             int w = e[in[v]].w;
41             if(w >= INF)return -1;
42             ans += Expand(e[in[v]].v , v) + w;
43         }
44     }
45     return ans;
46 }
47 ll Solve(int n , int m , int rt , Edge e[N + M])//filled e[1...m]
48 {
49     for(int i = 1 ; i <= n ; i++)e[++m] = {i % n + 1 , i , INF};
50     for(int i = 1 ; i <= m ; i++)pq[e[i].v].push(pr(e[i].w , i));
51     col.init(n * 2) , id.init(n * 2) , num = n;
52     for(int i = 1 ; i <= n ; i++)if(id[i] == i)Work(i);
53     return Expand(rt , num);
54 }

```

## 5.10 弦图

### 5.10.1 MCS 最大势算法。

---

```

1 // == Preparations ==
2 #include <vector>
3
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);
8 for (int i = 1, j = 0; i <= n; i++, j++) {
9     while (vec[j].empty()) j--;
10    int u = p[i] = vec[j].back();
11    vec[j].pop_back();
12    pos[u] = -1;
13    for (int k = g.hd[u]; k; k = g.nxt[k])
14        if (pos[g.to[k]] != -1) {
15            int v = g.to[k];
16            pos[vec[l[v]].back()] = pos[v];
17            swap(vec[l[v]][pos[v]], vec[l[v]].back());
18            vec[l[v]].pop_back();
19            pos[v] = vec[++l[v]].size();
20            vec[l[v]].push_back(v);
21        }
22 }
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  $c_1, c_2, \dots, c_k$ ，我们只需要判断  $c_1$  与  $c_j$  之间是否有边即可。因为这个团中其他边会在  $p_{c_2}, p_{c_3}, \dots, p_{c_k}$  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。

---

```

1 // == 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：

$$\begin{aligned}
 & \sum_{d_i \geq 1, \sum_{i=1}^k (d_i - 1) = k - 2} \binom{k - 2}{d_1 - 1, d_2 - 1, \dots, d_k - 1} \cdot \prod_{i=1}^k s_i^{d_i} \\
 &= \prod_{i=1}^k s_i \sum_{d_i \geq 1, \sum_{i=1}^k (d_i - 1) = k - 2} \binom{k - 2}{d_1 - 1, d_2 - 1, \dots, d_k - 1} \cdot \prod_{i=1}^k s_i^{d_i - 1} \\
 &= \left( \sum_{i=1}^k s_i \right)^{k-2} \prod_{i=1}^k s_i \\
 &= n^{k-2} \prod_{i=1}^k s_i
 \end{aligned}$$

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  $O(n)$ 。

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

令  $pre_i = \prod_{j=0}^i (k - j)$ ,  $suf_i = \prod_{j=i}^n (k - j)$ :

$$f(k) = \sum_{i=0}^n y_i \frac{pre_{i-1} \times suf_{i+1}}{i! \times (n-i)!} \times (-1)^{n-i}$$

重心拉格朗日插值:

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

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

则

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

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  $\sum_{i=0}^k \frac{t_i}{k - x_i}$  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  $G$  且  $G(F(x)) = 0$ ，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 ==
2 struct complex {
3     double a, b;
4
5     complex() = default;
6     complex(double _a, double _b): a(_a), b(_b) {}
7     complex operator+(const complex &x) const {return complex(a + x.a, b + x.b);}
8     complex operator-(const complex &x) const {return complex(a - x.a, b - x.b);}
9     complex operator*(const complex &x) const {return complex(a * x.a - b * x.b, a *
    ↪ x.b + b * x.a);}
10    complex operator/(const complex &x) const {
11        double t = b * b + x.b * x.b;
12        return complex((a * x.a + b * x.b) / t, (b * x.a - a * x.b) / t);
13    }
14    complex &operator+=(const complex &x) {return *this = *this + x;}
15    complex &operator-=(const complex &x) {return *this = *this - x;}
16    complex &operator*=(const complex &x) {return *this = *this * x;}

```

```

17     complex &operator/=(const complex &x) {return *this = *this / x;}
18 };
19 // == Main ==
20 void FFT(vector<complex> &f, int flag) const {
21     int n = f.size();
22     vector<int> swp(n);
23     for (int i = 0; i < n; i++) {
24         swp[i] = swp[i >> 1] >> 1 | ((i & 1) * (n >> 1));
25         if (i < swp[i]) std::swap(f[i], f[swp[i]]);
26     }
27     for (int mid = 1; mid < n; mid <= 1) {
28         complex w1(cos(pi / mid), flag * sin(pi / mid));
29         for (int i = 0; i < n; i += mid << 1) {
30             complex w(1, 0);
31             for (int j = 0; j < mid; j++, w *= w1) {
32                 complex x = f[i + j], y = w * f[i + mid + j];
33                 f[i + j] = x + y, f[i + mid + j] = x - y;
34             }
35         }
36     }
37     return;
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;
11         a = (long long)a * a % mod;
12         b >>= 1;
13     }
14     return ans % mod;
15 }
16
17 struct poly: vector<int> {
18     poly(initializer_list<int> &&arg): vector<int>(arg) {}
19     template<typename... argT>
20     poly(argT &&...args): vector<int>(forward<argT>(args)...) {}
21
22     poly operator+(const poly &b) const {
23         const poly &a = *this;
24         poly ans(max(a.size(), b.size()));
25         for (int i = 0; i < (int)ans.size(); i++)
26             ans[i] = ((i < (int)a.size() ? a[i] : 0) + (i < (int)b.size() ? b[i]
27                 ↪ : 0)) % mod;
28         return ans;
29     }
30     poly operator+=(const poly &b) {return *this = *this + b;}
31     poly operator-(const poly &b) const {
32         const poly &a = *this;
33         poly ans(max(a.size(), b.size()));
34         for (int i = 0; i < (int)ans.size(); i++)
35             ans[i] = ((i < (int)a.size() ? a[i] : 0) - (i < (int)b.size() ? b[i]
36                 ↪ : 0) + mod) % mod;
37         return ans;
38     }
39     poly operator--(const poly &b) {return *this = *this - b;}
40     void NTT(poly &g, int flag) const {
41         int n = g.size();
42         vector<unsigned long long> f(g.begin(), g.end());
43         vector<int> swp(n);
44         for (int i = 0; i < n; i++) {
45             swp[i] = swp[i >> 1] >> 1 | ((i & 1) * (n >> 1));
46             if (i < swp[i]) std::swap(f[i], f[swp[i]]);
47         }
48         for (int mid = 1; mid < n; mid <= 1) {
49             int w1 = power(flag ? G : invG, (mod - 1) / mid / 2);
50             vector<int> w(mid);
51             w[0] = 1;
52             for (int i = 1; i < mid; i++) w[i] = (long long)w[i - 1] * w1 % mod;
53             for (int i = 0; i < n; i += mid << 1)
54                 for (int j = 0; j < mid; j++) {
55                     int t = (long long)w[j] * f[i + mid + j] % mod;
56                     f[i + mid + j] = f[i + j] - t + mod;
57                     f[i + j] += t;
58                 }
59         }
60     }
61 }

```

```

57         if (mid == 1 << 10)
58             for (int i = 0; i < n; i++) f[i] %= mod;
59     }
60     int inv = flag ? 1 : power(n, mod - 2);
61     for (int i = 0; i < n; i++) g[i] = f[i] % mod * inv % mod;
62     return;
63 }
64
65 // 下面是基于转置原理的 NTT, 相对朴素版本效率更高。
66 void NTT(poly &g, int flag) const {
67     int n = g.size();
68     vector<int> f(g.begin(), g.end());
69     if (flag) {
70         for (int mid = n >> 1; mid >= 1; mid >>= 1) {
71             int w1 = power(G, (mod - 1) / mid / 2);
72             vector<int> w(mid);
73             w[0] = 1;
74             for (int i = 1; i < mid; i++) w[i] = (long long)w[i - 1] * w1 %
75                 ↪ mod;
76             for (int i = 0; i < n; i += mid << 1)
77                 for (int j = 0; j < mid; j++) {
78                     int t = (long long)(f[i + j] - f[i + mid + j] + mod) *
79                         ↪ w[j] % mod;
80                     f[i + j] = f[i + j] + f[i + mid + j] >= mod ?
81                         f[i + j] + f[i + mid + j] - mod : f[i + j] + f[i +
82                         ↪ mid + j];
83                     f[i + mid + j] = t;
84                 }
85             }
86             for (int i = 0; i < n; i++) g[i] = f[i];
87         } else {
88             for (int mid = 1; mid < n; mid <= 1) {
89                 int w1 = power(invG, (mod - 1) / mid / 2);
90                 vector<int> w(mid);
91                 w[0] = 1;
92                 for (int i = 1; i < mid; i++) w[i] = (long long)w[i - 1] * w1 %
93                     ↪ mod;
94                 for (int i = 0; i < n; i += mid << 1)
95                     for (int j = 0; j < mid; j++) {
96                         int t = (long long)w[j] * f[i + mid + j] % mod;
97                         f[i + mid + j] = f[i + j] - t < 0 ? f[i + j] - t + mod :
98                             ↪ f[i + j] - t;
99                         f[i + j] = f[i + j] + t >= mod ? f[i + j] + t - mod : f[i
100                         ↪ + j] + t;
101                     }
102             }
103             int inv = power(n, mod - 2);
104             for (int i = 0; i < n; i++) g[i] = (long long)f[i] * inv % mod;
105         }
106     }

```

```

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

```

```

148         for (int i = 0; i < len << 1; i++) g[i] = (long long)g[i] * g[i] %
            ↪ mod;
149         NTT(g, 0);
150         g += ff;
151         g *= tmp.inv();
152         g.resize(len);
153     }
154     g.resize(size());
155     return g;
156 }
157 poly derivative() const {
158     poly f(*this);
159     for (int i = 1; i < (int)f.size(); i++) f[i - 1] = (long long)f[i] * i %
            ↪ mod;
160     f.pop_back();
161     return f;
162 }
163 poly integral() const {
164     poly f(*this);
165     f.push_back(0);
166     for (int i = f.size() - 1; i >= 1; i--) f[i] = (long long)f[i - 1] *
            ↪ power(i, mod - 2) % mod;
167     f[0] = 0;
168     return f;
169 }
170 poly ln() const {
171     poly f((derivative() * inv()).integral());
172     f.resize(size());
173     return f;
174 }
175 poly exp() const { // 需要满足 F[0] = 0
176     poly f(*this), g;
177     g.push_back(1);
178     int n = 1;
179     while (n < (int)size()) n <<= 1;
180     f.resize(n);
181     for (int len = 2; len <= n; len <<= 1) {
182         poly tmp(g);
183         g.resize(len);
184         g = g.ln();
185         for (int i = 0; i < len; i++) g[i] = (f[i] - g[i] + mod) % mod;
186         g[0] = (g[0] + 1) % mod;
187         g *= tmp;
188         g.resize(len);
189     }
190     g.resize(size());
191     return g;
192 }
193 };

```

```

194
195 inline poly power(poly f, int b) { // 需要满足 F[0] = 1
196     f = f.ln();
197     for (int i = 0; i < (int)f.size(); i++) f[i] = (long long)f[i] * b % mod;
198     f = f.exp();
199     return f;
200 }
201 // 不要求 F[0] = 1 的多项式快速幂，但是我忘记怎么用了，记得去回顾一下！
202 poly power(poly f, int b1, int b2 = -1) {
203     if (b2 == -1) b2 = b1;
204     int n = f.size(), p = 0;
205     reverse(f.begin(), f.end());
206     while (!f.empty() && !f.back()) f.pop_back(), p++;
207     if (f.empty() || (long long)p * b1 >= n) return poly(n);
208     int v = f.back();
209     int inv = power(v, mod - 2);
210     for (int &i : f) i = (long long)i * inv % mod;
211     reverse(f.begin(), f.end());
212     f = f.ln();
213     for (int &i : f) i = (long long)i * b1 % mod;
214     f = f.exp();
215     reverse(f.begin(), f.end());
216     for (int i = 1; i <= p * b1; i++) f.push_back(0);
217     reverse(f.begin(), f.end());
218     f.resize(n);
219     v = power(v, b2);
220     for (int &i : f) i = (long long)i * v % mod;
221     return f;
222 }
223 }

```

---

## 6.6 FWT

```

1 void FWTor(int a[], int op) {
2     for (int l = 2; l <= n; l <= 1)
3         for (int i = 0; i < n; i += l)
4             for (int j = 0; j < l / 2; j++)
5                 a[i + j + l / 2] = (a[i + j + l / 2] + (long long)a[i + j] * op % mod
6                     ↪ + mod) % mod;
7     return;
8 }
9 void FWTand(int a[], int op) {
10     for (int l = 2; l <= n; l <= 1)
11         for (int i = 0; i < n; i += l)
12             for (int j = 0; j < l / 2; j++)

```

```

12         a[i + j] = (a[i + j] + (long long)a[i + j + l / 2] * op % mod + mod)
           ↪ % mod;
13     return;
14 }
15 void FWTxor(int a[], int op) {
16     for (int l = 2; l <= n; l <= 1)
17         for (int i = 0; i < n; i += l)
18             for (int j = 0; j < l / 2; j++) {
19                 int p = (a[i + j] + a[i + j + l / 2]) % mod, d = (a[i + j] - a[i + j
           ↪ + l / 2] + mod) % mod;
20                 a[i + j] = (long long)p * op % mod;
21                 a[i + j + l / 2] = (long long)d * op % mod;
22             }
23     return;
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);
10
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);}
13
14 // 向量 & 点
15 struct Vect {
16     double x, y;
17
18     Vect() = default;
19     Vect(double _x, double _y): x(_x), y(_y) {}
20     Vect operator+() const {return *this;}
21     Vect operator-() const {return Vect(-x, -y);}
22     Vect operator+(const Vect &b) const {return Vect(x + b.x, y + b.y);}
23     Vect operator-(const Vect &b) const {return Vect(x - b.x, y - b.y);}
24     Vect operator*(const double &t) const {return Vect(x * t, y * t);}
25     Vect operator/(const double &t) const {return Vect(x / t, y / t);}
26     double operator*(const Vect &b) const {return x * b.x + y * b.y;}
27     double operator^(const Vect &b) const {return x * b.y - y * b.x;}
28     Vect &operator+=(const Vect &b) {return *this = *this + b;}
29     Vect &operator-=(const Vect &b) {return *this = *this - b;}
30     Vect &operator*=(const double &t) {return *this = *this * t;}
31     Vect &operator/=(const double &t) {return *this = *this / t;}
```

```

32     bool operator==(const Vect &b) {return !sign(x - b.x) && !sign(y - b.y);}
33     double length() const {return sqrt(x * x + y * y);}
34     Vect normal() const {return *this / length();}
35 };
36 using Point = Vect;
37 // 多边形
38 struct Polygon: vector<Point> {
39     Polygon(initializer_list<Point> &&arg): vector<Point>(arg) {}
40     template<typename... argT>
41     explicit Polygon(argT &&...args): vector<Point>(forward<argT>(args)...) {}
42
43     // 多边形面积
44     double area() const {
45         double ans = 0;
46         for (int i = 0; i < (int)size(); i++) ans += (*this)[i] ^ (*this)[(i + 1) %
            ↪ size()];
47         return ans / 2;
48     }
49 };
50 // 直线
51 struct Line {
52     // 表示方式为起点 + 向量
53     Point s;
54     Vect dir;
55
56     Line() = default;
57     Line(Point _s, Vect _dir): s(_s), dir(_dir) {}
58 };
59 // 线段
60 struct Segment: Line {
61     Segment() = default;
62     Segment(Point _s, Vect _dir): Line(_s, _dir) {}
63 };
64 // 圆
65 struct Circle {
66     // 表示方式为圆心 + 半径
67     Point O;
68     double r;
69
70     Circle() = default;
71     Circle(Point _O, double _r): O(_O), r(_r) {}
72     double area() {return r * r * pi;}
73 };
74
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) /
    ↪ 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) {

```



```

79     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 -
    ↪ 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
86 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
88 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
96 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
100 inline int isOnSegment(Point a, Segment b) {
101     return isOnLine(a, b) && sign((a - b.s) * (a - b.s - b.dir)) <= 0;
102 }
103 // 判断直线 a 与线段 b 是否相交
104 inline int isIntersecting(Line a, Segment b) {
105     int va = sign((b.s - a.s) ^ a.dir), vb = sign((b.s + b.dir - a.s) ^ a.dir);
106     return !va || !vb || va != vb;
107 }
108 // 判断两条线段是否相交
109 inline int isIntersecting(Segment a, Segment b) {
110     return isOnSegment(b.s, a) || isOnSegment(b.s + b.dir, a) ||
111         isOnSegment(a.s, b) || isOnSegment(a.s + a.dir, b) ||
112         (sign((b.s - a.s) ^ a.dir) != sign((b.s + b.dir - a.s) ^ a.dir) &&
113         sign((a.s - b.s) ^ b.dir) != sign((a.s + a.dir - b.s) ^ b.dir));
114 }
115 // 直线交点
116 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
118 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) {
121     double ans = min(dist(a, b.s), dist(a, b.s + b.dir));
122     Point tmp = projection(a, b);
123     if (isOnSegment(tmp, b)) ans = min(ans, dist(a, tmp));

```

```

124     return ans;
125 }
126 // 线段间的距离
127 inline double dist(Segment a, Segment b) {
128     if (isIntersecting(a, b)) return 0;
129     return min({dist(a.s, b), dist(a.s + a.dir, b), dist(b.s, a), dist(b.s + b.dir,
        ↪ a)});
130 }
131 // 判断多边形是否是凸包
132 inline int isConvex(const Polygon &a) {
133     int n = a.size();
134     for (int i = 0; i < n; i++)
135         if (sign((a[(i + 1) % n] - a[i]) ^ (a[(i + 2) % n] - a[i])) < 0) return 0;
136     return 1;
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
139 inline int Containment(Point a, const Polygon &b) {
140     int n = b.size(), val = 0;
141     for (int i = 0; i < n; i++) {
142         Segment s = Segment(b[i], b[(i + 1) % n] - b[i]);
143         if (isOnSegment(a, s)) return 1;
144         int t = sign((b[(i + 1) % n] - b[i]) ^ (a - b[i]));
145         int va = sign(b[i].y - a.y), vb = sign(b[(i + 1) % n].y - a.y);
146         if (t > 0 && va <= 0 && vb > 0) val++;
147         if (t < 0 && vb <= 0 && va > 0) val--;
148     }
149     return val ? 2 : 0;
150 }
151 // 点集的凸包
152 inline Polygon Andrew(Polygon a) {
153     Polygon ans;
154     sort(a.begin(), a.end(), [](const Point &u, const Point &v) {
155         return u.x != v.x ? u.x < v.x : u.y < v.y;
156     });
157     ans.push_back(a[0]);
158     for (int i = 1; i < (int)a.size(); i++) {
159         while (ans.size() > 1) {
160             Point tmp = ans.back();
161             ans.pop_back();
162             if (sign((tmp - ans.back()) ^ (a[i] - tmp)) > 0) {ans.push_back(tmp);
                ↪ break;}
163         }
164         ans.push_back(a[i]);
165     }
166     int top = ans.size();
167     for (int i = (int)a.size() - 2; i >= 0; i--) {
168         while ((int)ans.size() > top) {
169             Point tmp = ans.back();

```

```

170         ans.pop_back();
171         if (sign((tmp - ans.back()) ^ (a[i] - tmp)) > 0) {ans.push_back(tmp);
            ↪ break;}
172     }
173     ans.push_back(a[i]);
174 }
175 ans.pop_back();
176 return ans;
177 }
178 // 两个凸包的闵可夫斯基和
179 inline Polygon Minkowski(Polygon l, Polygon r) {
180     Polygon diff1, diff2;
181     int siz1 = l.size(), siz2 = r.size();
182     for (int i = 1; i < siz1; i++) diff1.push_back(l[i] - l[i - 1]);
183     for (int i = 1; i < siz2; i++) diff2.push_back(r[i] - r[i - 1]);
184     Polygon ans;
185     ans.push_back(l[0] + r[0]);
186     int p1 = 0, p2 = 0;
187     while (p1 < siz1 - 1 && p2 < siz2 - 1)
188         if (sign(diff1[p1] ^ diff2[p2]) < 0) ans.push_back(ans.back() + diff1[p1++]);
189         else ans.push_back(ans.back() + diff2[p2++]);
190     while (p1 < siz1 - 1) ans.push_back(ans.back() + diff1[p1++]);
191     while (p2 < siz2 - 1) ans.push_back(ans.back() + diff2[p2++]);
192     return ans;
193 }
194 // 旋转卡壳求凸包直径
195 inline double Diameter(Polygon a) {
196     const int n = a.size();
197     if (n == 1) return 0;
198     if (n == 2) return dist(a[0], a[1]);
199     double ans = 0;
200     a.push_back(a[0]);
201     for (int i = 0, pos = 2; i < n; i++) {
202         Point u = a[i], v = a[i + 1];
203         ans = max(ans, dist(u, v));
204         while (sign(((u - a[pos + 1]) ^ (v - a[pos + 1])) - ((u - a[pos]) ^ (v -
            ↪ a[pos])))) >= 0)
205             pos = (pos + 1) % n;
206         ans = max({ans, dist(u, a[pos]), dist(v, a[pos])});
207     }
208     return ans;
209 }
210 // 扇形面积
211 inline double sector(double r, double rad) {return r * r * rad / 2;}
212 // 弧度为 rad 的弓形的面积
213 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) {

```

```

216     Line u(a, rotate(b - a, angle(b - a, c - a) / 2)), v(b, rotate(a - b, angle(a -
    ↪   b, c - b) / 2));
217     Circle ans;
218     ans.O = intersection(u, v);
219     ans.r = dist(ans.O, Line(a, b - a));
220     return ans;
221 }
222 // 三角形外接圆
223 inline Circle circumscribedCircle(Point a, Point b, Point c) {
224     Line u(middle(a, b), rotate(b - a, pi / 2)), v(middle(a, c), rotate(c - a, pi /
    ↪   2));
225     Circle ans;
226     ans.O = intersection(u, v);
227     ans.r = dist(ans.O, a);
228     return ans;
229 }
230 // 最小圆覆盖
231 inline Circle minimumCircle(Polygon a) {
232     mt19937 gen(chrono::system_clock::now().time_since_epoch().count());
233     int n = a.size();
234     shuffle(a.begin(), a.end(), gen);
235     Circle ans(Point(0, 0), 0);
236     for (int i = 0; i < n; i++)
237         if (sign(dist(ans.O, a[i]) - ans.r) > 0) {
238             ans = Circle(a[i], 0);
239             for (int j = 0; j < i; j++)
240                 if (sign(dist(ans.O, a[j]) - ans.r) > 0) {
241                     ans = Circle(middle(a[i], a[j]), dist(a[i], a[j]) / 2);
242                     for (int k = 1; k < j; k++)
243                         if (sign(dist(ans.O, a[k]) - ans.r) > 0)
244                             ans = circumscribedCircle(a[i], a[j], a[k]);
245                 }
246         }
247     return ans;
248 }
249 // 圆与直线的交点
250 inline pair<Point, Point> intersection(Circle a, Line b) {
251     Point p = projection(a.O, b);
252     double dis = dist(a.O, p);
253     dis = sqrt(a.r * a.r - dis * dis);
254     return {p - b.dir.normal() * dis, p + b.dir.normal() * dis};
255 }
256 // 两个圆的交点
257 inline pair<Point, Point> intersection(Circle a, Circle b) {
258     Vect u = b.O - a.O;
259     double rad = acos((a.r * a.r + u.length() * u.length() - b.r * b.r) / a.r /
    ↪   u.length() / 2);
260     u = u.normal() * a.r;
261     return {a.O + rotate(u, rad), a.O + rotate(u, -rad)};

```

```

262 }
263 // 点到圆的切点
264 inline pair<Point, Point> tangent(Point a, Circle b) {
265     double rad = asin(b.r / dist(b.O, a));
266     double dis = dist(b.O, a);
267     dis = sqrt(dis * dis - b.r * b.r);
268     Vect u = (b.O - a).normal() * dis;
269     return {a + rotate(u, -rad), a + rotate(u, rad)};
270 }
271 // 两个圆的公切线, 返回切点
272 inline vector<pair<Point, Point>> commonTangent(Circle a, Circle b) {
273     vector<pair<Point, Point>> ans;
274     double dis = dist(a.O, b.O);
275     if (sign(dis - fabs(a.r - b.r)) < 0) return ans;
276     else if (sign(dis - fabs(a.r - b.r)) == 0) {
277         ans.push_back(intersection(a, b));
278         return ans;
279     }
280     int flag = 0;
281     if (a.r < b.r) swap(a, b), flag = 1;
282     Vect u = (b.O - a.O).normal();
283     double rad = acos((a.r - b.r) / dis);
284     ans.emplace_back(a.O + rotate(u, rad) * a.r, b.O + rotate(-u, rad - pi) * b.r);
285     ans.emplace_back(a.O + rotate(u, -rad) * a.r, b.O + rotate(-u, pi - rad) * b.r);
286     if (sign(dis - a.r - b.r) >= 0) {
287         rad = acos((a.r + b.r) / dis);
288         if (sign(rad)) {
289             ans.emplace_back(a.O + rotate(u, rad) * a.r, b.O + rotate(-u, rad) *
290                 ↪ b.r);
291             ans.emplace_back(a.O + rotate(u, -rad) * a.r, b.O + rotate(-u, -rad) *
292                 ↪ b.r);
293         } else ans.emplace_back(a.O + u * a.r, b.O - u * b.r);
294     }
295     if (flag)
296         for (auto &i : ans) swap(i.first, i.second);
297     return ans;
298 }
299 // 两个圆的交的面积
300 inline double intersectionArea(Circle a, Circle b) {
301     int state = commonTangent(a, b).size();
302     if (state <= 1) return min(a.area(), b.area());
303     if (state >= 3) return 0;
304     pair<Point, Point> tmp = intersection(a, b);
305     double rada = fmod(angle(tmp.second - a.O, tmp.first - a.O) + 2 * pi, 2 * pi);
306     double radb = fmod(angle(tmp.first - b.O, tmp.second - b.O) + 2 * pi, 2 * pi);
307     return arch(a.r, rada) + arch(b.r, radb);
308 }

```

# 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>
4
5 mt19937 gen(chrono::system_clock::now().time_since_epoch().count());
6 mt19937_64 genll(chrono::system_clock::now().time_since_epoch().count());
7 // == Main ==
8 unsigned splitmix32(unsigned x) {
9     unsigned z = (x += 0x9E3779B9);
10    z = (z ^ (z >> 16)) * 0x85ebca6b;
11    z = (z ^ (z >> 13)) * 0xc2b2ae35;
12    return z ^ (z >> 16);
13 }
14
15 unsigned long long splitmix64(unsigned long long x) {
16    unsigned long long z = (x += 0x9e3779b97f4a7c15);
17    z = (z ^ (z >> 30)) * 0xbf58476d1ce4e5b9;
18    z = (z ^ (z >> 27)) * 0x94d049bb133111eb;
19    return z ^ (z >> 31);
20 }
21
22 struct custom_hash { // custom hash for unsigned long long
23     size_t operator()(unsigned long long x) const {
24         return splitmix64(x + genll());
25     }
26 };
27
28 struct custom_hash { // custom hash for pair<unsigned long long, unsigned long long>
29     size_t operator()(pair<unsigned long long, unsigned long long> x) const {
```

---

```

30         return (splitmix64(x.first + genll()) << 1) ^ splitmix64(x.second + genll());
31     }
32 };

```

---

## 8.1.2 xorshift

---

```

1 // == Main ==
2 unsigned long long xorshift(unsigned long long x) { x ^= x << 13; x ^= x >> 7; x ^= x
   ↪ << 17; return x; }
3 unsigned xorshift(unsigned x) { x ^= x << 13; x ^= x >> 17; x ^= x << 5; return x; }

```

---

## 8.1.3 手写哈希表

---

```

1 // == Main ==
2 template<typename ValType , typename KeyType>
3 struct HashTable
4 {
5     static const int M = 13075 , P = 13003; // P < M and P is between N^1.1 to N^1.7
6     struct Node{KeyType key; ValType v; int nxt;}e[M];
7     int tot , head[P];
8     inline void Add(int u , const KeyType& k , const ValType &v){e[++tot] = {k , v ,
   ↪ head[u]} , head[u] = tot;}
9     inline int hash(const KeyType& x){return x;}
10    ValType& operator[](const KeyType& x)
11    {
12        for(int i = head[hash(x) % P] ; i ; i = e[i].nxt)
13            if(e[i].key == x)return e[i].v;
14        Add(hash(x) % P , x , ValType());
15        return e[tot].v;
16    }
17    ValType at(const KeyType& x)
18    {
19        for(int i = head[hash(x) % P] ; i ; i = e[i].nxt)
20            if(e[i].key == x)return e[i].v;
21        return ValType();
22    }
23    void clear()
24    {
25        for(int i = 1 ; i <= tot ; i++)
26            head[hash(e[i].key) % P] = 0 , e[i] = {};
27        tot = 0;
28    }
29 };

```

---

## 8.2 取模类

---

```

1 // == Main ==
2 struct mint {
3     static const int mod = 998244353;
4     int v;
5
6     mint() = default;
7     mint(int _v): v((_v % mod + mod) % mod) {}
8     explicit operator int() const {return v;}
9     mint operator+(const mint &x) const {return v + x.v - (v + x.v < mod ? 0 : mod);}
10    mint &operator+=(const mint &x) {return *this = *this + x;}
11    mint operator-(const mint &x) const {return v - x.v + (v - x.v >= 0 ? 0 : mod);}
12    mint &operator-=(const mint &x) {return *this = *this - x;}
13    mint operator*(const mint &x) const {return (long long)v * x.v % mod;}
14    mint &operator*=(const mint &x) {return *this = *this * x;}
15    mint inv() const {
16        mint a(*this), ans(1);
17        int b(mod - 2);
18        while (b) {
19            if (b & 1) ans *= a;
20            a *= a;
21            b >>= 1;
22        }
23        return ans;
24    }
25    mint operator/(const mint &x) const {return *this * x.inv();}
26    mint &operator/=(const mint &x) {return *this = *this / x;}
27    mint operator-() {return mint(-v);}
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。

---

```

1 // == Main ==
2 struct Barrett {
3     unsigned long long b, m;
4     Barrett(unsigned long long b = 2): b(b), m((__uint128_t(1) << 64) / b) {}
5     unsigned long long reduce(long long x) {
6         unsigned long long r = (__uint128_t(x + b) * m) >> 64;
7         unsigned long long q = (x + b) - b * r;
8         return q >= b ? q - b : q;
9     }

```

---



```
10 } F;
```

## 8.3 对拍脚本

```
1  #!/usr/bin/bash
2
3  declare -i num=0
4
5  while [ true ]; do
6      ./mkdata > in.txt
7      time ./mine < in.txt > out.txt
8      ./correct < in.txt > ans.txt
9      diff out.txt ans.txt
10     if [ $? -ne 0 ]; then
11         echo "WA"
12         break
13     fi
14     num=num+1
15     echo "Passed $num tests."
16 done
```

## 8.4 VS Code 配置

### 8.4.1 User Tasks

```
1  {
2      // See https://go.microsoft.com/fwlink/?LinkId=733558
3      // for the documentation about the tasks.json format
4      "version": "2.0.0",
5      "tasks": [
6          {
7              "type": "shell",
8              "label": "My C++ Runner",
9              "detail": "Build and Run Current C++ Program",
10             "command": [ // 三个编译方式保留一个即可。
11                 "clear",
12                 "&&",
13                 "g++ ${file} -o ${fileDirname}/${fileBasenameNoExtension}
14                 ↪ -std=c++14 -Wall -Wextra && echo '== Normal ==',
15                 "g++ ${file} -o ${fileDirname}/${fileBasenameNoExtension}
16                 ↪ -std=c++14 -Wall -Wextra -O2 && echo '== O2 ==',
17                 "g++ ${file} -o ${fileDirname}/${fileBasenameNoExtension}
18                 ↪ -std=c++14 -Wall -Wextra -fsanitize=undefined,address && echo
19                 ↪ '== UB Check ==',
```

```

16         "&&",
17         "gnome-terminal -- bash -c \"ulimit -s 524288; time
    ↪   ${fileDirname}/${fileBasenameNoExtension}; read -p 'Press ENTER
    ↪   to continue...'; exit\""
18     ],
19     "problemMatcher": [ // 非必要
20         "$gcc"
21     ],
22     "group": { // 非必要
23         "kind": "build",
24         "isDefault": true
25     },
26     "presentation": { // 非必要
27         "showReuseMessage": false
28     }
29 }
30 ]
31 }

```

## 8.4.2 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:

```

1 {
2     "editor.fontSize": 16,
3     "editor.multiCursorModifier": "ctrlCmd",
4     "editor.insertSpaces": false,
5     "editor.acceptSuggestionOnEnter": "off",
6     "editor.rulers": [110],
7     "editor.cursorSmoothCaretAnimation": "on",
8     "window.commandCenter": false
9 }

```

### 8.4.3 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