Team Reference

Pollard

```
const int max_step = 4e5;
   unsigned long long gcd(unsigned long long a, unsigned long long b){
       if (!a) return 1;
       while (a) swap(a, b\%=a);
       return b;
   }
   unsigned long long get(unsigned long long a, unsigned long long b){
9
       if (a > b)
10
           return a-b;
11
       else
12
           return b-a;
13
   }
14
15
   unsigned long long pollard(unsigned long long n) {
16
       unsigned long long x = (rand() + 1) \% n, y = 1, g;
       int stage = 2, i = 0;
       g = gcd(get(x, y), n);
19
       while (g == 1){
20
           if (i == max_step)
21
               break;
           if (i == stage){
23
                y = x;
                stage <<= 1;
           }
           x = (x * (__int128)x + 1) \% n;
27
           i++;
28
           g = gcd(get(x, y), n);
29
       }
30
       return g;
31
   }
```

pragma

#pragma GCC optimize(''03,no-stack-protector'') #pragma GCC target(''sse,sse2,sse4,ssse3,popcnt,abm,mmx,avx,tune=native'')

Алгебра Pick

$$B + \Gamma / 2 - 1 = AREA,$$

где B — количество целочисленных точек внутри многоугольника, а Γ — количество целочисленных точек на границе многоугольника.

Newton

$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$$

Catalan
$$C_n = \sum_{k=0}^{n-1} C_k C_{n-1-k}$$

$$C_i = \frac{1}{n+1} {2n \choose n}$$

Кол-во графов

$$G_N := 2^{n(n-1)/2}$$

Количество связных помеченных графов

$$Conn_N = G_N - \frac{1}{N} \sum_{K=1}^{N-1} K\binom{N}{K} Conn_K G_{N-K}$$

Количество помеченных графов с К компонентами связности

$$D[N][K] = \sum_{S=1}^{N} {N-1 \choose S-1} Conn_S D[N-S][K-1]$$

Miller-Rabbin

Интегрирование по формуле Симпсона

$$\int_{a}^{b} f(x)dx?$$

$$x_{i} := a + ih, i = 0 \dots 2n$$

$$h = \frac{b-a}{2n}$$

$$\int_{O(n^4)} (f(x_0) + 4f(x_1) + 2f(x_2) + 4f(x_3) + 2f(x_4) + \dots + 4f(x_{2n-1}) + f(x_{2n}))) \frac{h}{3}$$

Простые числа

1009,1013;10007,10009;100003,100019 1000003,1000033;10000019,10000079 100000007,100000037 10000000019,10000000033 100000000039,100000000061

$10000000000031, 10000000000067 \\ 1000000000000061, 1000000000000069 \\ 1000000000000000003, 100000000000000009$

Числа для Фурье

- prime: $7340033 = 7 \cdot 2^{20} + 1; w : 5(w^{2^{20}} = 1)$
- prime: $13631489 = 13 \cdot 2^{20} + 1$; $w: 3(w^{2^{20}} = 1)$
- prime: $23068673 = 11 \cdot 2^{21} + 1$; $w: 38(w^{2^{21}} = 1)$
- prime: $69206017 = 33 \cdot 2^{21} + 1$; $w: 45(w^{2^{21}} = 1)$
- prime: $81788929 = 39 \cdot 2^{21} + 1$; $w: 94(w^{2^{21}} = 1)$
- prime: $104857601 = 25 \cdot 2^{22} + 1$; $w : 21(w^{2^{22}} = 1)$
- prime: $113246209 = 27 \cdot 2^{22} + 1$; $w : 66(w^{2^{22}} = 1)$
- prime: $138412033 = 33 \cdot 2^{22} + 1$; $w: 30(w^{2^{22}} = 1)$
- prime: $167772161 = 5 \cdot 2^{25} + 1$; $w : 17(w^{2^{25}} = 1)$
- prime: $469762049 = 7 \cdot 2^{26} + 1$; $w: 30(w^{2^{26}} = 1)$
- prime: $998244353 = 7 \cdot 17 \cdot 2^{23} + 1$; $w: 3^{7*17}$.

```
/** Begin fast allocation */
   const int MAX_MEM = 5e8;
   int mpos = 0;
   /** End fast allocation */
   #define pb push_back
  #define mp make_pair
  #define fst first
  #define snd second
   #define ll long long
   #define forn(i, n) for (int i = 0; i < (int) (n); i++)
   \#define\ forlr(i,\ l,\ r)\ for\ (int\ i=(int)\ l;\ i <=(int)\ (r);\ i++)
   \#define\ forrl(i,\ r,\ l)\ for\ (int\ i=(int)\ r;\ i>=(int)\ (l);\ i--)
15
16
   /** Interface */
17
   inline int readChar();
   template <class T = int> inline T readInt();
20
   template <class T> inline void writeInt( T x, char end = 0 );
21
   inline void writeChar( int x );
   inline void writeWord( const char *s );
23
   /** Read */
   static const int buf_size = 2048;
27
28
   inline int getChar() {
29
       static char buf[buf_size];
30
       static int len = 0, pos = 0;
       if (pos == len)
           pos = 0, len = fread(buf, 1, buf_size, stdin);
       if (pos == len)
           return -1;
35
       return buf[pos++];
   }
37
   inline int readWord(char * buffer) {
       int c = getChar();
40
       while (c <= 32) {
41
           c = getChar();
42
       }
44
       int len = 0;
       while (c > 32) {
           *buffer = (char) c;
           c = getChar();
           buffer++;
49
           len++;
       }
```

```
return len;
53
   inline int readChar() {
        int c = getChar();
        while (c \le 32)
57
            c = getChar();
       return c;
60
   template <class T>
   inline T readInt() {
        int s = 1, c = readChar();
64
        T x = 0;
65
        if (c == '-')
            s = -1, c = getChar();
        while ('0' <= c && c <= '9')
            x = x * 10 + c - 0, c = getChar();
       return s == 1 ? x : -x;
   }
71
72
   /** Write */
73
74
   static int write_pos = 0;
75
   static char write_buf[buf_size];
   inline void writeChar( int x ) {
78
        if (write_pos == buf_size)
79
            fwrite(write_buf, 1, buf_size, stdout), write_pos = 0;
       write_buf[write_pos++] = x;
81
   }
82
   template <class T>
   inline void writeInt( T x, char end ) {
85
        if (x < 0)
            writeChar('-'), x = -x;
        char s[24];
        int n = 0;
        while (x \mid | !n)
            s[n++] = 0 + x \% 10, x /= 10;
        while (n--)
93
            writeChar(s[n]);
        if (end)
95
            writeChar(end);
   }
97
98
   inline void writeWord( const char *s ) {
99
        while (*s)
100
            writeChar(*s++);
101
   }
102
```

```
struct treap{
       map<char, int> go;
       int len, suff;
       long long sum_in;
       treap(){}
   };
   treap v[max_n * 4];
   int last = 0;
   int add_treap(int max_len){
11
       v[number].sum_in = 0;
12
       v[number].len = max_len;
13
       v[number].suff = -1;
14
       number++;
       return number - 1;
16
   }
17
   void add_char(char c){
       int cur = last;
20
       int new_treap = add_treap(v[cur].len + 1);
21
       last = new_treap;
22
       while (\operatorname{cur} != -1){
23
           if (v[cur].go.count(c) == 0){
                v[cur].go[c] = new_treap;
                v[new_treap].sum_in += v[cur].sum_in;
                cur = v[cur].suff;
                if (cur == -1)
                    v[new_treap].suff = 0;
           }else{
                int a = v[cur].go[c];
                if (v[a].len == v[cur].len + 1){
                    v[new_treap].suff = a;
                }else{
                    int b = add_treap(v[cur].len + 1);
                    v[b].go = v[a].go;
                    v[b].suff = v[a].suff;
                    v[new_treap].suff = b;
                    while (cur != -1 && v[cur].go.count(c) != 0 && v[cur].go[c] == a){
                        v[cur].go[c] = b;
                        v[a].sum_in -= v[cur].sum_in;
                        v[b].sum_in += v[cur].sum_in;
42
                        cur = v[cur].suff;
                    v[a].suff = b;
                }
                return;
           }
48
       }
49
  }
50
```

```
int k = sqrt((double)p) + 2;
   for (int i = k; i >= 1; i--)
       mp[bin(b, (i * 111 * k) \% (p-1), p)] = i;
  bool answered = false;
   int ans = INT32_MAX;
   for (int i = 0; i \le k; i++){
       int sum = (n * 111 * bin(b, i, p)) % p;
       if (mp.count(sum) != 0){
10
           int an = mp[sum] * 111 * k - i;
           if (an < p)
12
               ans = min(an, ans);
13
       }
15 }
```

```
int gcd (int a, int b, int & x, int & y) {
           if (a == 0) {
                    x = 0; y = 1;
                    return b;
           }
           int x1, y1;
           int d = gcd (b\%a, a, x1, y1);
           x = y1 - (b / a) * x1;
           y = x1;
           return d;
10
  }
11
  const int N = 10000000;
   int lp[N+1];
   vector<int> pr;
   for (int i=2; i<=N; ++i) {</pre>
           if (lp[i] == 0) {
                    lp[i] = i;
                    pr.push_back (i);
           }
           for (int j=0; j<(int)pr.size() && pr[j]<=lp[i] && i*pr[j]<=N; ++j)</pre>
                    lp[i * pr[j]] = pr[j];
  }
12
```

```
fill(par, par + 301, -1);
   fill(par2, par2 + 301, -1);
   int ans = 0;
   for (int v = 0; v < n; v++){
       memset(useda, false, sizeof(useda));
       memset(usedb, false, sizeof(usedb));
       useda[v] = true;
       for (int i = 0; i < n; i++)
           w[i] = make_pair(a[v][i] + row[v] + col[i], v);
       memset(prev, 0, sizeof(prev));
       int pos;
       while (true){
13
           pair<pair<int, int>, int> p = make_pair(make_pair(1e9, 1e9), 1e9);
14
           for (int i = 0; i < n; i++)
               if (!usedb[i])
16
                   p = min(p, make_pair(w[i], i));
           for (int i = 0; i < n; i++)
               if (!useda[i])
                   row[i] += p.first.first;
           for (int i = 0; i < n; i++)
21
               if (!usedb[i]){
22
                    col[i] -= p.first.first;
23
                   w[i].first -= p.first.first;
           ans += p.first.first;
           usedb[p.second] = true;
           prev[p.second] = p.first.second; //из второй в первую
28
           int x = par[p.second];
           if (x == -1){
30
               pos = p.second;
               break;
           }
           useda[x] = true;
           for (int j = 0; j < n; j++)
35
               w[j] = min(w[j], \{a[x][j] + row[x] + col[j], x\});
37
       while (pos != -1){
           int nxt = par2[prev[pos]];
           par[pos] = prev[pos];
41
           par2[prev[pos]] = pos;
42
           pos = nxt;
       }
44
   }
45
   cout << ans << ''\n'';
   for (int i = 0; i < n; i++)
47
       cout << par[i] + 1 << "" " << i + 1 << "\n";
48
```

```
struct edge{
       int from, to;
       int c, f, num;
       edge(int from, int to, int c, int num):from(from), to(to), c(c), f(0),
       num(num){}
       edge(){}
   };
   const int max_n = 600;
   edge eds[150000];
   int num = 0;
   int it[max_n];
   vector<int> gr[max_n];
   int s, t;
   vector<int> d(max_n);
   bool bfs(int k){
       queue<int> q;
       q.push(s);
19
       fill(d.begin(), d.end(), -1);
20
       d[s] = 0;
       while (!q.empty()){
22
           int v = q.front();
           q.pop();
           for (int x : gr[v])
                if (d[eds[x].to] == -1 \&\& eds[x].c - eds[x].f >= (1 << k)){
                    d[eds[x].to] = d[v] + 1;
27
                    q.push(eds[x].to);
               }
29
       }
       return (d[t] != -1);
   }
33
34
   int dfs(int v, int flow, int k){
35
       if (flow < (1 << k))
36
           return 0;
       if (v == t)
           return flow;
       for (; it[v] < gr[v].size(); it[v]++){</pre>
40
           if (d[v] + 1 != d[eds[gr[v][it[v]]].to])
41
               continue;
           int num = gr[v][it[v]];
43
           int res = dfs(eds[gr[v][it[v]]].to, min(flow, eds[gr[v][it[v]]].c -
       eds[gr[v][it[v]]].f), k);
           if (res){
45
                eds[num].f += res;
46
               eds[num ^1].f -= res;
47
               return res;
           }
49
```

```
}
50
       return 0;
51
   }
52
53
   void add(int fr, int to, int c, int nm){
54
       gr[fr].push_back(num);
55
       eds[num++] = edge(fr, to, c, nm);
56
       gr[to].push_back(num);
       eds[num++] = edge(to, fr, 0, nm); //corrected c
   }
59
60
   int ans = 0;
61
       for (int k = 30; k >= 0; k--)
62
           while (bfs(k)){
63
                memset(it, 0, sizeof(it));
                while (int res = dfs(s, 1e9 + 500, k))
                    ans += res;
           }
   // decomposition
70
   int path_num = 0;
   vector<int> paths[550];
73
   int flows[550];
   int decomp(int v, int flow){
76
       if (flow < 1)
77
           return 0;
       if (v == t){
79
           path_num++;
           flows[path_num - 1] = flow;
           return flow;
       }
       for (int i = 0; i < gr[v].size(); i++){</pre>
           int num = gr[v][i];
           int res = decomp(eds[num].to, min(flow, eds[num].f));
           if (res){
                eds[num].f -= res;
                paths[path_num - 1].push_back(eds[num].num);
                return res;
90
           }
91
       }
       return 0;
93
   }
94
   while (decomp(s, 1e9 + 5));
```

```
long long ans = 0;
   int mx = 2 * n + 2;
  memset(upd, 0, sizeof(upd));
   for (int i = 0; i < mx; i++)
       dist[i] = inf;
  dist[st] = 0;
   queue<int> q;
  q.push(st);
   upd[st] = 1;
10
   while (!q.empty()){
       int v = q.front();
       q.pop();
13
       if (upd[v]){
14
           for (int x : gr[v])
                                         {
                edge &e = edges[x];
16
                if (e.c - e.f > 0 \&\& dist[v] != inf \&\& dist[e.to] > dist[v] + e.w) {
                    dist[e.to] = dist[v] + e.w;
                    if (!upd[e.to])
                        q.push(e.to);
20
                    upd[e.to] = true;
21
                    p[e.to] = x;
22
                }
23
           }
24
           upd[v] = false;
       }
   }
27
28
   for (int i = 0; i < k; i++){
29
       for (int i = 0; i < mx; i++)</pre>
30
           d[i] = inf;
       d[st] = 0;
       memset(used, false, sizeof(used));
       set<pair<int, int> > s;
       s.insert(make_pair(0, st));
35
       for (int i = 0; i < mx; i++){
           int x;
37
           while (!s.empty() && used[(s.begin() -> second)]){
                s.erase(s.begin());
           }
           if (s.empty())
41
                break;
42
           x = s.begin() -> second;
43
           used[x] = true;
44
           s.erase(s.begin());
           for (int i = 0; i < gr[x].size(); i++){
                edge &e = edges[gr[x][i]];
                if (!used[e.to] \&\& e.c - e.f > 0){
                    if (d[e.to] > d[x] + (e.c - e.f) * e.w + dist[x] - dist[e.to]){}
49
                        d[e.to] = d[x] + (e.c - e.f) * e.w + dist[x] - dist[e.to];
50
                        p[e.to] = gr[x][i];
51
```

```
s.insert(make_pair(d[e.to], e.to));
52
                    }
53
                }
           }
           dist[x] += d[x];
       }
57
       int pos = t;
       while (pos != st){
                int id = p[pos];
60
                edges[id].f += 1;
           edges[id ^ 1].f -= 1;
           pos = edges[id].from;
       }
64
   }
65
```

}

```
string min_cyclic_shift (string s) {
           s += s;
           int n = (int) s.length();
           int i=0, ans=0;
           while (i < n/2) {
                    ans = i;
                    int j=i+1, k=i;
                    while (j < n \&\& s[k] <= s[j]) {
                            if (s[k] < s[j])
                                     k = i;
                             else
                                     ++k;
                            ++j;
14
                    while (i <= k)
                                     i += j - k;
           }
16
           return s.substr (ans, n/2);
17
  }
      Sum over subsets
  for(int i = 0; i<(1<<N); ++i)</pre>
           F[i] = A[i];
  for(int i = 0; i < N; ++i) for(int mask = 0; mask < (1<<N); ++mask){
           if(mask & (1<<i))</pre>
                    F[mask] += F[mask^(1<< i)];
```

```
vector<int> getZ(string s){
       vector<int> z;
       z.resize(s.size(), 0);
       int 1 = 0, r = 0;
       for (int i = 1; i < s.size(); i++){</pre>
            if (i <= r)
                z[i] = min(r - i + 1, z[i - 1]);
            while (i + z[i] < s.size() \&\& s[z[i]] == s[i + z[i]])
                z[i]++;
            if (i + z[i] - 1 > r){
                r = i + z[i] - 1;
                1 = i;
            }
13
       }
14
       return z;
15
   }
16
17
   vector<int> getP(string s){
       vector<int> p;
       p.resize(s.size(), 0);
20
       int k = 0;
21
       for (int i = 1; i < s.size(); i++){</pre>
22
            while (k > 0 \&\& s[i] == s[k])
23
                k = p[k - 1];
            if (s[i] == s[k])
                k++;
            p[i] = k;
28
       return p;
29
   }
30
   vector<int> getH(string s){
32
       vector<int> h;
33
       h.resize(s.size() + 1, 0);
34
       for (int i = 0; i < s.size(); i++)</pre>
35
            h[i + 1] = ((h[i] * 111 * pow) + s[i] - 'a' + 1) \% mod;
       return h;
37
   }
38
   int getHash(vector<int> &h, int 1, int r){
40
       int res = (h[r + 1] - h[1] * p[r - 1 + 1]) \% mod;
41
       if (res < 0)
42
            res += mod;
43
       return res;
44
   }
45
```

suf array + lcp

43 }

```
char *s; // входная строка
   int n; // длина строки
   const int maxlen = ...; // максимальная длина строки
   const int alphabet = 256; // pasmep andaeuma, <= maxlen
   int p[maxlen], cnt[maxlen], c[maxlen];
   memset (cnt, 0, alphabet * sizeof(int));
   for (int i=0; i<n; ++i)
           ++cnt[s[i]];
   for (int i=1; i<alphabet; ++i)</pre>
           cnt[i] += cnt[i-1];
   for (int i=0; i<n; ++i)</pre>
12
           p[--cnt[s[i]]] = i;
13
   c[p[0]] = 0;
14
   int classes = 1;
   for (int i=1; i<n; ++i) {
           if (s[p[i]] != s[p[i-1]]) ++classes;
           c[p[i]] = classes-1;
   }
19
   //
20
   int pn[maxlen], cn[maxlen];
21
   for (int h=0; (1<<h)<n; ++h) {
22
           for (int i=0; i<n; ++i) {</pre>
23
                    pn[i] = p[i] - (1 << h);
                    if (pn[i] < 0) pn[i] += n;
           }
26
           memset (cnt, 0, classes * sizeof(int));
           for (int i=0; i<n; ++i)</pre>
28
                    ++cnt[c[pn[i]]];
           for (int i=1; i < classes; ++i)</pre>
                    cnt[i] += cnt[i-1];
           for (int i=n-1; i>=0; --i)
                    p[--cnt[c[pn[i]]]] = pn[i];
           cn[p[0]] = 0;
           classes = 1;
           for (int i=1; i<n; ++i) {
                    int mid1 = (p[i] + (1 << h)) \% n, mid2 = (p[i-1] + (1 << h)) \% n;
                    if (c[p[i]] != c[p[i-1]] || c[mid1] != c[mid2])
                             ++classes;
                    cn[p[i]] = classes-1;
40
41
           memcpy (c, cn, n * sizeof(int));
42
```

```
//p[i] -- prefix (id of first symbol) on i-th position of suff array (from 0)
  for (int i = 0; i < n; i++)
       r[p[i]] = i;
   int k = 0;
  for (int j = 0; j < n; j++){
       int i = r[j];
       k--;
       if (k < 0 | | i == n - 1)
           k = 0;
       if (i != n - 1)
10
           while (s[p[i] + k] == s[p[i + 1] + k])
               k++;
       lcp[i] = k;
13
   }
14
  for (int i = 0; i + 1 < n; i++)</pre>
15
       cout << lcp[i] << "";
```

```
int num = 0;
   long long phi = n, nn = n;
   for (long long x:primes){
       if (x*x>nn)
           break;
       if (nn \% x == 0){
           while (nn \% x == 0)
                nn /= x;
           phi -= phi/x;
           num++;
       }
   }
   if (nn != 1){
13
       phi -= phi/nn;
14
       num++;
15
   }
16
   if (!((num == 1 && n % 2 != 0) || n == 4 || n == 2 || (num == 2 && n % 2 == 0 && n
       % 4 != 0))){
       cout << "-1\n";
       continue;
19
20
   vector<long long> v;
21
   long long pp = phi;
   for (long long x:primes){
       if (x*x>pp)
           break;
       if (pp \% x == 0){
26
           while (pp \% x == 0)
27
                pp /= x;
           v.push_back(x);
       }
   }
31
   if (pp != 1){
       v.push_back(pp);
33
34
   while (true){
35
       long long a = primes[rand()%5000]%n;
36
       if (gcd(a, n) != 1)
           continue;
       bool bb = false;
       for (long long x:v)
           if (pow(a, phi/x) == 1){
                bb = true;
                break;
           }
       if (!bb){
           cout << a << ''\n'';
46
           break;
47
       }
48
   }
49
```

```
int log = 20;
   int N = 1 \ll log;
   typedef complex<double> cd;
   int rev[N];
   cd root[N];
   void init() {
       for (int i = 0; i != N; ++i)
10
           rev[i] = (rev[i >> 1] >> 1) + ((i & 1) << (maxlog - 1));
       const double pi = acos(-1);
       for (int k = 1; k < maxn; k *= 2) {
           cd tmp(pi / k);
           root[k] = \{1, 0\};
           for (int i = 1; i < k; i++)
               root[k + i] = (i \& 1) ? root[(k + i) >> 1] * tmp : root[(k + i) >> 1];
       }
   }
20
21
   void fft(vector<cd>& a) {
22
       for (int i = 0; i != N; ++i)
23
           if (rev[i] < i)
               swap(res[rev[i]], res[i]);
       for (int k = 1; k < maxn; k *= 2)
           for (int i = 0; i < maxn; i += 2 * k)
               for (int j = 0; j != k; ++j) {
                    cd tmp = root[k + j] * res[i + j + k];
                   res[i + j + k] = res[i + j] - tmp;
                   res[i + j]
                               = res[i + j] + tmp;
               }
   }
34
   void inv fft(vector<cd>& a) {
35
       fft(a);
       reverse(a.begin() + 1, a.end());
37
       for (cd& elem: a)
           elem /= N;
   }
41
   void fast_fourier(vector<int>& a) { // AND-FFT.
       for (int k = 1; k < SZ(a); k *= 2)
           for (int start = 0; start < (1 << K); start += 2 * k) {
               for (int off = 0; off < k; ++off) {</pre>
                   int a_val = a[start + off];
                   int b_val = a[start + k + off];
                   a[start + off] = b_val;
                   a[start + k + off] = add(a_val, b_val);
```

```
}
10
           }
11
   }
12
   void inverse_fast_fourier(vector<int>& a) {
14
       for (int k = 1; k < SZ(a); k *= 2)
15
           for (int start = 0; start < (1 << K); start += 2 * k) {</pre>
16
                for (int off = 0; off < k; ++off) {</pre>
                    int a_val = a[start + off];
                    int b_val = a[start + k + off];
                    a[start + off] = sub(b_val, a_val);
                    a[start + k + off] = a_val;
                }
23
           }
  }
25
```

 $\mathbf{D}\mathrm{M}$

Кол-во корневых деревьев:

$$t(G) = \frac{1}{n}\lambda_2 \dots \lambda_n \ (\lambda_1 = 0)$$

Кол-во эйлеровых циклов:

$$e(D) = t^-(D,x) \cdot \prod_{y \in D} (outdeg(y) - 1)!$$

Наличие совершенного паросочетания:

T — матрица с нулями на диагонали. Если есть ребро (i,j), то $a_{i,j}:=x_{i,j},\ a_{j,i}=-x_{i,j}$ $\det(T)=0\Leftrightarrow$ нет совершенного паросочетания.

Whitespace code FFT