

```

1 #include "../bits/stdc++.h"
2 /**
3  * FFT における  $\omega = \exp(-2\pi i/N)$  を  $\omega^N = 1 \pmod{P}$ 
4  * となるような 1 の原始 n 乗根に拡張
5  *
6  *  $\text{sum}_{\{k=0\}^{n-1}\{\omega^{((1-j)*k)}\}} = (l==j) ? n : 0$ 
7  *
8  * e.g.  $P = 998244353 = 7 * 17 * 2^{23} + 1 \rightarrow \omega = 3, 31\dots$ 
9  *  $P = 163577857 = 39 * 2^{22} + 1 \rightarrow 23\dots$ 
10  *  $P = 167772161 = 5 * 2^{25} + 1 \rightarrow 3,\dots$ 
11  *  $P = 469762049 = 7 * 2^{26} + 1 \rightarrow 3,\dots$ 
12  *
13  * E に対する n-1 次多項式 f を定義する. (n は 2 の冪乗)
14  *  $f(E) = a_{n-1}E^{n-1} + \dots + a_1E + a_0$ 
15  *
16  * NTT における順変換
17  *  $f_k = a_{n-1}\omega^{(n-1)k} + \dots + a_1\omega^k + a_0$ 
18  *  $= \text{sum}_{\{l=0\}^{n-1}\{a_l\omega^{lk}\}} \quad (k = 0, 1, \dots, n-1)$ 
19  * となる  $f_k$  を求める
20  *
21  * 逆変換
22  *  $a_j = (1/n) * \text{sum}_{\{k=0\}^{n-1}\{f_k\omega^{-kj}\}} \quad (j = 0, 1, \dots, n-1)$ 
23  */
24 // verified: http://judge.u-aizu.ac.jp/onlinejudge/review.jsp?rid=3384943
25 class NTT
26 {
27     using ll = long long;
28     // mod = 998244353
29     const int mod = 7 * 17 * (1 << 23) + 1;
30
31     static const int omega_max = 23;
32     static const int root = 31;
33     std::vector<int> omega;
34
35     int mod_inv(ll a, ll m)
36     {
37         ll b = mod, u = 1, v = 0;
38         while (b > 0)
39         {
40             ll t = a / b;
41             a -= t * b;
42             std::swap(a, b);
43             u -= t * v;
44             std::swap(u, v);
45         }
46         return (u % m + m) % m;
47     }
48     std::vector<int> fft(std::vector<int> v, bool inv)
49     {
50         const int n = v.size();
51         // assert(n == 2^冪);
52         int _logn = 0;
53         while ((1 << _logn) < n)
54             _logn++;
55         assert(1 << _logn == n);
56         int ww = omega[_logn];
57         if (inv)
58             ww = mod_inv(ww, mod);
59         for (int m = n; m >= 2; m >>= 1)
60         {
61             const int mh = m >> 1;
62             int w = 1;
63             for (int i = 0; i < mh; i++)
64             {
65                 for (int j = i; j < n; j += m)
66                 {
67                     const int k = j + mh;
68                     int x = v[j] - v[k];
69                     if (x < 0)
70                         x += mod;
71                     v[j] += v[k];
72                     if (v[j] >= mod)
73                         v[j] -= mod;
74                     v[k] = (1LL * w * x) % mod;
75                 }
76                 w = (1LL * w * ww) % mod;
77             }
78             ww = (1LL * ww * ww) % mod;
79         }
80
81         int i = 0;
82         for (int j = 1; j < n - 1; j++)
83         {
84             for (int k = n >> 1; k > (i ^ k); k >>= 1)
85                 ;
86             if (j < i)
87                 std::swap(v[i], v[j]);
88         }
89         if (inv)
90         {
91             const int inv_n = mod_inv(n, mod);
92             for (auto &x : v)
93             {
94                 x = (1LL * x * inv_n) % mod;
95             }
96         }
97     }
98 }

```

```
96     }
97     return v;
98 }
99
100 public:
101     NTT()
102     {
103         omega.resize(omega_max + 1);
104         int x = root;
105         for (int i = omega_max; i >= 0; i--)
106         {
107             omega[i] = x;
108             x = (1LL * x * x) % mod;
109         }
110     }
111     std::vector<int> convolution(std::vector<int> f, std::vector<int> g)
112     {
113         int sz = 1;
114         const int m = f.size() + g.size() - 1;
115         while (sz < m)
116             sz *= 2;
117         f.resize(sz), g.resize(sz);
118         f = this->fft(std::move(f), false);
119         g = this->fft(std::move(g), false);
120         for (int i = 0; i < sz; i++)
121         {
122             f[i] = (1LL * f[i] * g[i]) % mod;
123         }
124         return this->fft(std::move(f), true);
125     }
126 };
127
128 /**
129  * 任意 mod 拡張
130  * 異なる mod で NTT を複数回計算し, Garner のアルゴリズムを適用する
131  * 2^30 程度なら一意に結果を復元できる
132  */
133
```