# Содержание

1	Setup & Scripts         1.1 CMake          1.2 wipe.sh          1.3 Builtins	1 1 1 2
2	$\mathbf{G}++$ builtins	2
3	Bugs	2
4	Geometry         4.1 Пересечение прямых	<b>3</b>
5	Numbers	3
6	Graphs 6.1 Weighted matroid intersection	<b>3</b>
7	Push-free segment tree	6
8	Number theory  8.1 Chinese remainder theorem without overflows	7 7 8
9	Suffix Automaton	8
10	Smth added at last moment  10.1 Dominator Tree	9 11 13 14
11	Karatsuba	16
1	Setup & Scripts	
1.	1 CMake	
	ake_minimum_required(VERSION 3.14) oject(olymp)	
ad #s	t(CMAKE_CXX_STANDARD 17) d_compile_definitions(LOCAL) et(CMAKE_CXX_FLAGS "\${CMAKE_CXX_FLAGS} -fsanitize=undefined -fno → sanitize-recover") anitizers: address, leak, thread, undefined, memory	0-
ad	<pre>d_executable(olymp f.cpp)</pre>	

# 1.2 wipe.sh

```
1 touch {a..l}.cpp
2
3 for file in ?.cpp ; do
4    cat template.cpp > $file ;
5 done
```

#### 1.3 Builtins

### 2 G++ builtins

- \_\_builtin\_popcount(x) количество единичных бит в двоичном представлении 32-битного (знакового или беззнакового) целого числа.
- \_\_builtin\_popcountll(x) то же самое для 64-битных типов.
- \_\_builtin\_ctz(x) количество нулей на конце двоичного представления 32-битного целого числа. Например, для 5 вернётся 0, для 272 = 256 + 16 4 и т. д. Может не работать для нуля (вообще не стоит вызывать для x = 0, по-моему это и упасть может).
- $\bullet$  builtin ctzll(x) то же самое для 64-битных типов.
- \_\_builtin\_clz(x) количество нулей в начале двоичного представления 32-битного целого числа. Например, для  $2^{31}$  или  $-2^{31}$  вернётся 0, для 1 31 и т. д. Тоже не надо вызвывать с x = 0.
- $\bullet$  builtin clzll(x) то же самое для 64-битных типов.
- bitset<N>.\_Find\_first() номер первой позиции с единицей в битсете или его размер (то есть N), если на всех позициях нули.
- $\bullet$  bitset<N>.\_Find\_next(x) номер первой позиции с единицей среди позиций с номерами строго больше x; если такой нет, то N.

## 3 Bugs

- powmod:)
- Всегда чекать Куна дважды, особенно на количество итераций
- uniform int distribution от одного параметра
- for (char c : "NEWS")
- Порядок верхних и нижних границ в случае, когда задача двумерна  $t-b \neq b-t$
- static с мультитестами
- set со своим компаратором склеивает элементы

## 4 Geometry

### 4.1 Пересечение прямых

$$AB = A - B; CD = C - D$$
 
$$(A \times B \cdot CD.x - C \times D \cdot AB.x : A \times B \cdot CD.y - C \times D \cdot AB.y : AB \times CD)$$

#### 5 Numbers

• A lot of divisors

$$- \leq 20 : d(12) = 6$$

$$- \leq 50 : d(48) = 10$$

$$- \leq 100 : d(60) = 12$$

$$- \leq 1000 : d(840) = 32$$

$$- \leq 10^4 : d(9240) = 64$$

$$- \leq 10^5 : d(83160) = 128$$

$$- \leq 10^6 : d(720720) = 240$$

$$- \leq 10^7 : d(8648640) = 448$$

$$- \leq 10^8 : d(91891800) = 768$$

$$- \leq 10^9 : d(931170240) = 1344$$

$$- \leq 10^{11} : d(97772875200) = 4032$$

$$- \leq 10^{12} : d(963761198400) = 6720$$

$$- \leq 10^{15} : d(866421317361600) = 26880$$

$$- \leq 10^{18} : d(897612484786617600) = 103680$$

• Numeric integration

- simple: 
$$F(0)$$
  
- simpson:  $\frac{F(-1)+4\cdot F(0)+F(1)}{6}$   
- runge2:  $\frac{F(-\sqrt{\frac{1}{3}})+F(\sqrt{\frac{1}{3}})}{2}$   
- runge3:  $\frac{F(-\sqrt{\frac{3}{5}})\cdot 5+F(0)\cdot 8+F(\sqrt{\frac{3}{5}})\cdot 5}{18}$ 

## 6 Graphs

### 6.1 Weighted matroid intersection

```
// here we use T = __int128 to store the independent set
// calling expand k times to an empty set finds the maximum
// cost of the set with size exactly k,
// that is independent in blue and red matroids
// ver is the number of the elements in the matroid,
// e[i].w is the cost of the i-th element
```

```
7 // first return value is new independent set
8 // second return value is difference between
9 // new and old costs
10 // oracle(set, red) and oracle(set, blue) check whether
11 // or not the set lies in red or blue matroid respectively
12
13 auto expand = [\&B] (T cur set) \rightarrow pair<T, int>
14 {
       vector<int> in(ver);
15
       for (int i = 0; i < ver; i++)
16
            in[i] = ((cur_set >> i) & 1);
17
18
19
       const int red = 1;
20
       const int blue = 2;
21
       vector<vector<int>>> g(ver);
22
       for (int i = 0; i < ver; i++)
23
       for (int j = 0; j < ver; j++)
24
25
           T swp_mask = (cur_set ^(T(1) << i) ^(T(1) << j));
26
           if (!in[i] & in[j])
27
28
                if (oracle(swp_mask, red))
29
                    g[i].push back(j);
30
                if (oracle(swp_mask, blue))
31
                    g[j].push back(i);
32
33
           }
       }
34
35
36
       vector<int> from, to;
       for (int i = 0; i < ver; i++) if (!in[i])</pre>
37
38
           T add mask = cur set ^(T(1) \ll i);
39
           if (oracle(add mask, blue))
40
                from.push_back(i);
41
           if (oracle(add_mask, red))
42
                to.push back(i);
43
       }
44
45
       auto get cost = [\delta] (int x)
46
47
           const int cost = (!in[x] ? e[x].w : -e[x].w);
48
           return (ver + 1) * cost - 1;
49
       };
50
51
52
       const int inf = int(1e9);
53
       vector<int> dist(ver, -inf), prev(ver, -1);
       for (int x : from)
54
           dist[x] = get_cost(x);
55
56
```

```
57
        queue<int> q;
58
        vector<int> used(ver);
59
        for (int x : from)
60
61
62
             q.push(x);
             used[x] = 1;
63
        }
64
65
        while (!q.empty())
66
67
             int cur = q.front(); used[cur] = 0; q.pop();
68
69
             for (int to : g[cur])
70
71
                 int cost = get_cost(to);
72
                 if (dist[to] < dist[cur] + cost)</pre>
73
74
75
                      dist[to] = dist[cur] + cost;
                      prev[to] = cur;
76
                      if (!used[to])
77
78
                          used[to] = 1;
79
                          q.push(to);
80
                      }
81
82
                 }
83
             }
        }
84
85
86
        int best = -inf, where = -1;
        for (int x : to)
87
88
             if (dist[x] > best)
89
90
91
                 best = dist[x];
92
                 where = x;
             }
93
        }
94
95
96
        if (best = -inf)
             return pair<T, int>(cur_set, best);
97
98
        while (where \neq -1)
99
100
             cur_set ^= (T(1) \ll where);
101
             where = prev[where];
102
103
104
        while (best % (ver + 1))
105
106
             best++;
```

```
best \neq (ver + 1);
107
108
         assert(oracle(cur_set, red) & oracle(cur_set, blue));
109
        return pair<T, int>(cur_set, best);
110
111 };
    7
        Push-free segment tree
 1 class pushfreesegtree
 2
 3
         vector<modulo♦> pushed, unpushed;
 4
        modulo ⇔ add(int l, int r, int cl, int cr, int v, const modulo
 5
            \leftrightarrow \Leftrightarrow \&x)
         {
 6
             if (r \le cl || cr \le l)
 7
 8
                 return 0;
 9
             if (l \leq cl \& cr \leq r)
 10
                 unpushed[v] += x;
 11
 12
                 return x * (cr - cl);
 13
             }
14
15
             int ct = (cl + cr) / 2;
 16
 17
             auto tmp = add(l, r, cl, ct, 2 * v, x) + add(l, r, ct, cr,
18
                \rightarrow 2 * v + 1, x);
19
20
             pushed[v] += tmp;
21
22
             return tmp;
         }
23
24
25
        modulo ⇔ sum(int l, int r, int cl, int cr, int v)
26
27
         {
             if (r \leq cl || cr \leq l)
28
29
                 return 0:
             if (l \le cl \& cr \le r)
30
                 return pushed[v] + unpushed[v] * (cr - cl);
31
32
             int ct = (cl + cr) / 2;
33
34
35
             return sum(l, r, cl, ct, 2 * v) + unpushed[v] * (min(r, cr)
                \rightarrow - max(l, cl)) + sum(l, r, ct, cr, 2 * v + 1);
         }
36
37
    public:
38
        pushfreesegtree(int n): pushed(2 * up(n)), unpushed(2 * up(n))
39
```

```
{}
40
41
42
       modulo ⇒ sum(int l, int r)
43
44
45
            return sum(l, r, 0, pushed.size() / 2, 1);
       }
46
47
48
       void add(int l, int r, const modulo ♦ &x)
49
50
            add(l, r, 0, pushed.size() / 2, 1, x);
51
52
53 };
```

### 8 Number theory

#### 8.1 Chinese remainder theorem without overflows

```
1 // Replace T with an appropriate type!
2 using T = long long;
3
4 // Finds x, y such that ax + by = gcd(a, b).
  T gcdext (T a, T b, T &x, T &y)
5
6
  {
7
       if (b = 0)
8
9
            x = 1, y = 0;
10
            return a;
11
12
       T res = gcdext(b, a \% b, y, x);
13
14
       y -= x * (a / b);
15
       return res;
  }
16
17
18 // Returns true if system x = r1 \pmod{m1}, x = r2 \pmod{m2} has
      → solutions
   // false otherwise. In first case we know exactly that x = r \pmod{m}
19
      \rightarrow )
20
   bool crt (T r1, T m1, T r2, T m2, T &r, T &m)
22
   {
23
       if (m2 > m1)
24
25
            swap(r1, r2);
26
            swap(m1, m2);
       }
27
28
29
       T g = \underline{gcd(m1, m2)};
```

```
30
       if ((r2 - r1) \% g \neq 0)
31
           return false;
32
33
       T c1, c2;
34
       auto nrem = gcdext(m1 / g, m2 / g, c1, c2);
35
       assert(nrem = 1);
       assert(c1 * (m1 / g) + c2 * (m2 / g) = 1);
36
37
       T a = c1;
       a *= (r2 - r1) / g;
38
       a \% = (m2 / g);
39
       m = m1 / g * m2;
40
       r = a * m1 + r1;
41
42
       r = r \% m;
       if (r < 0)
43
44
           r += m;
45
       assert(r % m1 = r1 \& r % m2 = r2);
46
47
       return true;
48 }
   8.2 Integer points under a rational line
1 // integer (x, y) : 0 \le x < n, 0 < y \le (kx + b) / d
2 // (real division)
3 // In other words, sum_{x=0}^{n-1} [(kx+b)/d]
4 ll trapezoid (ll n, ll k, ll b, ll d)
5 {
       if (k = 0)
6
           return (b / d) * n;
7
       if (k \ge d || b \ge d)
8
           return (k / d) * n * (n - 1) / 2 + (b / d) * n + trapezoid(
9
              \rightarrow n, k % d, b % d, d);
       return trapezoid((k * n + b) / d, d, (k * n + b) % d, k);
10
11 }
   9
       Suffix Automaton
1 struct Vx{
2
       static const int AL = 26;
       int len, suf;
3
       int next[AL];
4
       Vx(){}
5
       Vx(int l, int s):len(l), suf(s){}
6
7
  };
8
9 struct SA{
       static const int MAX_LEN = 1e5 + 100, MAX_V = 2 * MAX_LEN;
10
       int last, vcnt;
11
       Vx v[MAX V];
12
13
14
       SA(){
```

```
15
           vcnt = 1;
16
           last = newV(0, 0); // root = vertex with number 1
17
       int newV(int len, int suf){
18
           v[vcnt] = Vx(len, suf);
19
20
           return vcnt++;
       }
21
22
       int add(char ch){
23
           int p = last, c = ch - 'a';
24
           last = newV(v[last].len + 1, 0);
25
           while(p & !v[p].next[c]) //added p &
26
                v[p].next[c] = last, p = v[p].suf;
27
           if(!p)
28
                v[last].suf = 1;
29
30
           else{
                int q = v[p].next[c];
31
                if (v[q].len = v[p].len + 1)
32
                    v[last].suf = q;
33
                else{
34
                    int r = newV(v[p].len + 1, v[q].suf);
35
                    v[last].suf = v[q].suf = r;
36
                    memcpy(v[r].next, v[q].next, sizeof(v[r].next));
37
                    while(p & v[p].next[c] = q)
38
                        v[p].next[c] = r, p = v[p].suf;
39
                }
40
41
42
           return last;
       }
43
44 };
```

### 10 Smth added at last moment

#### 10.1 Dominator Tree

```
1 struct dom_tree {
     vvi g, rg, tree, bucket;
2
     vi sdom, par, dom, dsu, label, in, order, tin, tout;
3
     int T = 0, root = 0, n = 0;
4
5
     void dfs tm (int x) {
6
       in[x] = T;
7
       order[T] = x;
8
       label[T] = T, sdom[T] = T, dsu[T] = T, dom[T] = T;
9
       T++;
10
11
       for (int to : g[x]) {
         if (in[to] = -1) {
12
           dfs tm(to);
13
           par[in[to]] = in[x];
14
         }
15
```

```
rg[in[to]].pb(in[x]);
16
        }
17
     }
18
19
     void dfs_tree (int v, int p) {
20
21
        tin[v] = T ++;
        for (int dest : tree[v]) {
22
          if (dest \neq p) {
23
            dfs_tree(dest, v);
24
25
        }
26
27
       tout[v] = T;
28
29
     dom_tree (const vvi &g_, int root_) {
30
31
        g = g_{;}
        n = sz(g);
32
33
        assert(0 \leq \text{root } \delta \delta \text{root } < n);
        in.assign(n, -1);
34
35
        rg.resize(n);
        order = sdom = par = dom = dsu = label = vi(n);
36
37
        root = root_;
        bucket.resize(n);
38
        tree.resize(n);
39
40
        dfs tm(root);
41
42
        for (int i = n - 1; i \ge 0; i--) {
43
          for (int j : rg[i])
44
45
            sdom[i] = min(sdom[i], sdom[find(j)]);
          if (i > 0)
46
            bucket[sdom[i]].pb(i);
47
48
49
          for (int w : bucket[i]) {
            int v = find(w);
50
            dom[w] = (sdom[v] = sdom[w] ? sdom[w] : v);
51
          }
52
53
          if (i > 0)
54
55
            unite(par[i], i);
        }
56
57
        for (int i = 1; i < n; i++) {
58
          if (dom[i] \neq sdom[i])
59
            dom[i] = dom[dom[i]];
60
          tree[order[i]].pb(order[dom[i]]);
61
62
          tree[order[dom[i]]].pb(order[i]);
        }
63
64
65
       T = 0;
```

```
66
       tin = tout = vi(n);
67
       dfs_tree(root, -1);
68
69
     void unite (int u, int v) {
70
71
       dsu[v] = u;
72
73
     int find (int u, int x = 0) {
74
       if (u = dsu[u])
75
         return (x ? -1 : u);
76
       int v = find(dsu[u], x + 1);
77
78
       if (v = -1)
79
         return u;
       if (sdom[label[dsu[u]]] < sdom[label[u]])</pre>
80
         label[u] = label[dsu[u]];
81
82
       dsu[u] = v;
       return (x ? v : label[u]);
83
84
85
     bool dominated_by (int v, int by_what) {
86
       return tin[by_what] ≤ tin[v] & tout[v] ≤ tout[by_what];
87
88
     }
89 };
   10.2
         Suffix Array
1 namespace suff arr {
2
3 const int MAXN = 2e5 + 10;
4
5 string s;
6 int n;
7 int p[MAXN];
8 int lcp[MAXN];
9 int pos[MAXN];
10 int c[MAXN];
11
12 void print() {
13 #ifndef LOCAL
14
       return;
15 #endif
       eprintf("p:\n");
16
17
       forn(i, sz(s)) {
           eprintf("i=%d -- %d: %s, lcp=%d, c=%d\n", i, p[i], s.substr
18
              \hookrightarrow (p[i], sz(s) - p[i]).data(), lcp[i], c[p[i]]);
19
20
       eprintf("\n");
21
  }
22
23 void build(const string& s_) {
```

```
static int cnt[MAXN];
24
25
       static int np[MAXN];
       static int nc[MAXN];
26
27
28
       s = s_{;}
29
       n = sz(s);
30
       memset (cnt, 0, sizeof cnt);
31
       for (char ch : s) {
32
            ++cnt[int(ch)];
33
       }
34
35
       forn(i, 256) {
            cnt[i + 1] += cnt[i];
36
37
       forn(i, sz(s)) {
38
            p[--cnt[int(s[i])]] = i;
39
       }
40
41
42
       int cls = 1;
       c[p[0]] = cls - 1;
43
       for (int i = 1; i < n; ++i) {
44
            if (s[p[i]] \neq s[p[i-1]]) {
45
                ++cls;
46
47
            c[p[i]] = cls - 1;
48
       }
49
50
       for (int len = 1; len ≤ n; len *= 2) {
51
            memset (cnt, 0, sizeof(int) * cls);
52
53
            forn(i, n) {
                ++cnt[c[i]];
54
55
            forn(i, cls - 1) {
56
                cnt[i + 1] += cnt[i];
57
58
            ford(i, n) {
59
                const int j = p[i];
60
                int j2 = (j - len + n) % n;
61
                np[--cnt[c[j2]]] = j2;
62
63
            memcpy(p, np, sizeof(int) * n);
64
65
            cls = 1;
66
            nc[p[0]] = cls - 1;
67
            for (int i = 1; i < n; ++i) {
68
                if (c[p[i]] \neq c[p[i-1]] || c[(p[i] + len) % n] \neq c
69
                   \rightarrow [(p[i - 1] + len) % n]) {
70
                    ++cls;
71
72
                nc[p[i]] = cls - 1;
```

```
73
           memcpy(c, nc, sizeof(int) * n);
74
       }
75
76
       forn(i, n) {
77
           pos[p[i]] = i;
78
79
80
       int pref = 0;
81
       forn(i, n) {
82
           int pi = pos[i];
83
           if (pi = n - 1) {
84
               continue;
85
86
           int j = p[pi + 1];
87
           while (i + pref < n \&\& j + pref < n \&\&\& s[i + pref] = s[j +
88
              → pref]) {
                ++pref;
89
90
           lcp[pi] = pref;
91
92
           pref = max(0, pref - 1);
       }
93
94
             print();
95 //
96 }
97
98 };
   10.3 Fast LCS
1 // assumes that strings consist of lowercase latin letters
2 const int M = ((int)1e5 + 64) / 32 * 32;
3 // maximum value of m
4 using bs = bitset<M>;
5 using uint = unsigned int;
6 const ll bnd = (1LL << 32);
7
8 // WARNING: invokes undefined behaviour of modifying ans through
      → pointer to another data type (uint)
9 // seems to work, but be wary
10 bs sum (const bs &bl, const bs &br)
11 {
       const int steps = M / 32;
12
13
       const uint* l = (uint*)&bl;
       const uint* r = (uint*)&br;
14
15
16
       bs ans;
17
       uint* res = (uint*)&ans;
18
       int carry = 0;
19
       forn (i, steps)
20
```

```
{
21
22
           ll cur = ll(*l++) + ll(*r++) + carry;
           carry = (cur ≥ bnd);
23
           cur = (cur ≥ bnd ? cur - bnd : cur);
24
           *res++ = uint(cur);
25
26
       }
27
28
       return ans;
29 }
30
31 int fast_lcs (const string &s, const string &t)
32 {
33
       const int m = sz(t);
       const int let = 26;
34
35
36
       vector<bs> has(let);
       vector<bs> rev = has;
37
38
39
       forn (i, m)
40
           const int pos = t[i] - 'a';
41
           has[pos].set(i);
42
            forn (j, let) if (j \neq pos)
43
                rev[j].set(i);
44
       }
45
46
47
       bs row;
       forn (i, m)
48
           row.set(i);
49
50
       int cnt = 0;
51
       for (char ch : s)
52
53
           const int pos = ch - 'a';
54
55
           bs next = sum(row, row & has[pos]) | (row & rev[pos]);
56
           cnt += next[m];
57
           next[m] = 0;
58
59
60
           row = next;
       }
61
62
63
       return cnt;
64 }
   10.4 Fast Subset Convolution
1 // algorithm itself starts here
void mobius (int* a, int n, int sign)
3 {
4
       forn (i, n)
```

```
{
5
           int free = ((1 << n) - 1) ^ (1 << i);
6
           for (int mask = free; mask > 0; mask = ((mask - 1) & free))
7
                (sign = +1 ? add : sub)(a[mask ^ (1 << i)], a[mask]);
8
9
           add(a[1 << i], a[0]);
       }
10
   }
11
12
13 // maximum number of bits allowed
14 const int B = 20;
15
16 vi fast conv (vi a, vi b)
17 {
       assert(!a.empty());
18
       const int bits = __builtin_ctz(sz(a));
19
       assert(sz(a) = (1 \ll bits) \& sz(a) = sz(b));
20
21
       static int trans a[B + 1][1 \ll B];
22
23
       static int trans b[B + 1][1 \ll B];
       static int trans_res[B + 1][1 << B];</pre>
24
25
       forn (cnt, bits + 1)
26
27
       {
           for (auto cur : {trans_a, trans_b, trans_res})
28
                fill(cur[cnt], cur[cnt] + (1 \ll bits), 0);
29
       }
30
31
       forn (mask, 1 << bits)
32
33
           const int cnt = __builtin_popcount(mask);
34
           trans_a[cnt][mask] = a[mask];
35
           trans_b[cnt][mask] = b[mask];
36
       }
37
38
       forn (cnt, bits + 1)
39
40
           mobius(trans a[cnt], bits, +1);
41
           mobius(trans_b[cnt], bits, +1);
42
       }
43
44
       // Not really a valid ranked mobius transform! But algorithm
45
          → works anyway
46
       forn (i, bits + 1) forn (j, bits - i + 1) forn (mask, 1 \ll bits
47
          \hookrightarrow )
           add(trans_res[i + j][mask], mult(trans_a[i][mask], trans_b[
48
              \rightarrow j][mask]));
49
       forn (cnt, bits + 1)
50
           mobius(trans_res[cnt], bits, -1);
51
```

```
52
53
       forn (mask, 1 << bits)
54
       {
           const int cnt = __builtin_popcount(mask);
55
           a[mask] = trans_res[cnt][mask];
56
57
       }
58
59
       return a;
60
  }
        Karatsuba
   11
1 // functon Karatsuba (and stupid as well) computes c += a * b, not
      \hookrightarrow c = a * b
2
3 using hvect = vector<modulo♦>::iterator;
  using hcvect = vector<modulo♦>::const iterator;
5
6
7 void add(hcvect abegin, hcvect aend, hvect ans)
8 {
       for (auto it = abegin; it \neq aend; +it, +ans)
9
           *ans += *it;
10
  }
11
12
13
14 void sub(hcvect abegin, hcvect aend, hvect ans)
15
       for (auto it = abegin; it \neq aend; +it, +ans)
16
           *ans -= *it;
17
   }
18
19
20
21 void stupid(int siz, hcvect abegin, hcvect bbegin, hvect ans)
22 {
       for (auto a = abegin; a \neq abegin + siz; +a, ans -= (siz - 1))
23
           for (auto b = bbegin; b \neq bbegin + siz; ++b, ++ans)
24
25
                *ans += *a * *b;
26
   }
27
28
  void Karatsuba(size_t siz, hcvect abegin, hcvect bbegin, hvect ans,
29
      → hvect small, hvect big, hvect sum)
30 {
       assert((siz & (siz - 1)) = \emptyset);
31
32
       if (siz \leq 32)
33
34
           stupid(siz, abegin, bbegin, ans);
35
36
```

```
37
           return;
       }
38
39
       auto amid = abegin + siz / 2, aend = abegin + siz;
40
       auto bmid = bbegin + siz / 2, bend = bbegin + siz;
41
       auto smid = sum + siz / 2, send = sum + siz;
42
43
       fill(small, small + siz, 0);
44
       Karatsuba(siz / 2, abegin, bbegin, small, small + siz, big +
45
          \hookrightarrow siz, sum);
       fill(big, big + siz, 0);
46
       Karatsuba(siz / 2, amid, bmid, big, small + siz, big + siz, sum
47
48
       copv(abegin, amid, sum);
49
       add(amid, aend, sum);
50
51
       copy(bbegin, bmid, sum + siz / 2);
       add(bmid, bend, sum + siz / 2);
52
53
54
       Karatsuba(siz / 2, sum, smid, ans + siz / 2, small + siz, big +
          \rightarrow siz, send);
55
       add(small, small + siz, ans);
56
       sub(small, small + siz, ans + siz / 2);
57
       add(big, big + siz, ans + siz);
58
       sub(big, big + siz, ans + siz / 2);
59
60 }
61
62
63 void mult(vector<modulo♦> a, vector<modulo♦> b, vector<modulo♦>
      → &c)
64 {
       a.resize(up(max(a.size(), b.size())), 0);
65
       b.resize(a.size(), 0);
66
67
       c.assign(a.size() * 2, 0);
68
69
70
       auto small = c;
71
       auto big = c;
72
       auto sum = c;
73
       Karatsuba(a.size(), a.begin(), b.begin(), c.begin(), small.
74
          → begin(), big.begin(), sum.begin());
75 }
```







