UPLB Eliens - Pegaraw Notebook

Contents

D 1 C1 1

1	Data	a Structures	1							
	1.1	Union Find	1							
2	Dynamic Programming									
	2.1	Edit Distance	1							
	2.2	Knapsack	1							
	2.3	Longest Common Subsequence	1							
	2.4	Longest Increasing Subsequence	1							
	2.5	Subset Sum	1							
3	Gra	ph Theory	2							
	3.1	Articulation Point	2							
	3.2	Bellman Ford	2							
	3.3	Bridge	2							
	3.4	Dijkstra	2							
	3.5	Floyd Warshall	2							
	3.6	Hierholzer	2							
	3.7	Is Bipartite	3							
	3.8	Is Cyclic	3							
	3.9	Kahn	3							
	3.10	Maximum Bipartite Matching	3							
	3.11	Max Flow	3							
	3.12	Prim Mst	3							
	3.13	Strongly Connected Component	4							
	3.14	Topological Sort	4							
4	Nun	nber Theory	4							
	4.1	Extended Euclidean	4							
	4.2	Find All Solutions	4							
	4.3	Linear Sieve	4							
	4.4	Miller Rabin	5							
	4.5	Modulo Inverse	5							
	4.6	Pollard Rho Brent	5							
	4.7	Range Sieve	5							
	4.8	Segmented Sieve	5							
	4.9	Tonelli Shanks	5							

1 Data Structures

1.1 Union Find

```
class UF {
    private: vi p;
        UF(int N) {p.assign(N, -1);}
        int fs(int i) {return (p[i] < 0) ? i : (p[i] =
              fs(p[i]));}
        bool isSame(int i, int j) {return fs(i) == fs(j
            );}
        void join(int i, int j) {
            int x = fs(i), y = fs(j);
            if (!(x == y)){
                if (x < y) \{ p[x] += p[y]; p[y] = x; \}
                else {p[y] += p[x]; p[x] = y; } }
12 };
```

2 Dynamic Programming

2.1 Edit Distance

```
11 edit_distance(string x, string y, 11 n, 11 m) {
  vector<vector<int>> dp(n + 1, vector<int>(m + 1,
       INF));
  dp[0][0] = 0;
  for (int i = 1; i <= n; i++) {</pre>
    dp[i][0] = i;
  for (int j = 1; j \le m; j++) {
    dp[0][j] = j;
  for (int i = 1; i <= n; i++) {</pre>
    for (int j = 1; j <= m; j++) {</pre>
      dp[i][j] = min({dp[i - 1][j] + 1, dp[i][j -
           1] + 1, dp[i - 1][j - 1] + (x[i - 1] !=
           y[j - 1])));
  return dp[n][m];
```

2.2 Knapsack

```
1 11 knapsack(11 W, vector<11> &wt, vector<11> &val,
        11 n) {
     vector<11> dp(W + 1, 0);
     for (11 i = 1; i <= n; i++) {
       for (11 w = W; w >= 0; w--) {
         if (wt[i - 1] <= w) {</pre>
            dp[w] = max(dp[w], dp[w - wt[i - 1]] + val[
                <u>i</u> - 1]);
8
9
     return dp[W];
```

2.3 Longest Common Subsequence

```
1 11 LCS(string x, string y, 11 n, 11 m) {
    vector<vector<ll>>> dp(n + 1, vector<ll>(m + 1));
     for (11 i = 0; i <= n; i++) {
      for (ll j = 0; j <= m; j++) {
         if (i == 0 || j == 0) {
           dp[i][j] = 0;
         } else if (x[i - 1] == y[j - 1]) {
           dp[i][j] = dp[i - 1][j - 1] + 1;
           dp[i][j] = max(dp[i - 1][j], dp[i][j - 1]);
     ll index = dp[n][m];
     vector<char> lcs(index + 1);
     lcs[index] = ' \setminus 0';
     11 i = n, j = m;
     while (i > 0 \&\& j > 0) {
      if (x[i-1] == y[j-1]) {
```

lcs[index - 1] = x[i - 1];

```
i--;
          index--;
        } else if (dp[i - 1][j] > dp[i][j - 1]) {
        } else {
      return dp[n][m];
31 }
```

2.4 Longest Increasing Subsequence

```
1  ll get_ceil_idx(vector<ll> &a, vector<ll> &T, ll 1,
        11 r, 11 x) {
     while (r - 1 > 1) {
       11 m = 1 + (r - 1) / 2;
       if (a[T[m]] >= x) {
       } else {
     return r;
   11 LIS(11 n, vector<11> &a) {
     11 len = 1;
     vector<11> T(n, 0), R(n, - 1);
     T[0] = 0;
     for (11 i = 1; i < n; i++) {
      if (a[i] < a[T[0]]) {</pre>
       T[0] = i;
      } else if (a[i] > a[T[len - 1]]) {
       R[i] = T[len - 1];
         T[len++] = i;
       } else {
         ll pos = get_ceil_idx(a, T, -1, len - 1, a[i
         R[i] = T[pos - 1];
         T[pos] = i;
     return len;
```

2.5 Subset Sum

```
bool subset_sum(ll n, vector<ll> &arr, ll sum) {
  vector<vector<ll>> dp(n + 1, vector<ll>(sum + 1,
       false));
  dp[0][0] = true;
  for (ll i = 1; i <= n; i++) {
    for (11 j = 0; j <= sum; j++) {
      dp[i][j] = dp[i - 1][j];
      if (j >= arr[i]) {
        dp[i][j] = dp[i - 1][j - arr[i]];
  return dp[n][sum];
```

3 Graph Theory

3.1 Articulation Point

```
void APUtil(vector<vector<ll>>> &adj, ll u, vector<</pre>
         bool> &visited,
    vector<ll> &disc, vector<ll> &low, 11 &time, 11
         parent, vector<bool> &isAP) {
      11 children = 0;
      visited[u] = true;
      disc[u] = low[u] = ++time;
      for (auto v : adj[u]) {
        if (!visited[v]) {
          children++;
 9
          APUtil(adj, v, visited, disc, low, time, u,
               isAP):
          low[u] = min(low[u], low[v]);
11
          if (parent != -1 && low[v] >= disc[u]) {
12
            isAP[u] = true;
13
14
        } else if (v != parent) {
15
          low[u] = min(low[u], disc[v]);
16
      if (parent == -1 && children > 1) {
19
        isAP[u] = true;
20
21
    void AP(vector<vector<11>>> &adj, 11 n) {
23
      vector<ll> disc(n), low(n);
24
      vector<bool> visited(n), isAP(n);
25
      11 time = 0, par = -1;
26
      for (11 u = 0; u < n; u++) {
        if (!visited[u]) {
28
          APUtil(adj, u, visited, disc, low, time, par,
                isAP);
29
      for (11 u = 0; u < n; u++) {</pre>
        if (isAP[u]) {
          cout << u << " ";
34
```

3.2 Bellman Ford

```
void bellman_ford(vector<vector<ll>>> &edges, ll n,
         ll m, ll src, vector<ll> &dis) {
      for (11 i = 0; i < n; i++) {
        dis[i] = INF;
      for (11 i = 0; i < n - 1; i++) {
         for (11 j = 0; j < m; j++) {
          11 u = edges[j][0], v = edges[j][1], w =
               edges[j][2];
          if (dis[u] < INF) {</pre>
             dis[v] = min(dis[v], dis[u] + w);
11
12
13
      for (11 i = 0; i < m; i++) {
14
         11 u = edges[i][0], v = edges[i][1], w = edges[
             i][2];
```

3.3 Bridge

```
void bridge_util(vector<vector<ll>>> &adj, ll u,
         vector<bool> &visited, vector<ll> &disc,
         vector<ll> &low, vector<ll> &parent) {
      static 11 time = 0;
      visited[u] = true;
      disc[u] = low[u] = ++time;
      list<ll>::iterator i;
      for (auto v : adj[u]) {
       if (!visited[v]) {
 8
          parent[v] = u;
 9
          bridge_util(adj, v, visited, disc, low,
              parent);
          low[u] = min(low[u], low[v]);
          if (low[v] > disc[u]) {
            cout << u << ' ' << v << '\n';
        } else if (v != parent[u]) {
          low[u] = min(low[u], disc[v]);
18
    void bridge(vector<vector<ll>> &adj, ll n) {
     vector<bool> visited(n, false);
      vector<ll> disc(n), low(n), parent(n, -1);
      for (11 i = 0; i < n; i++) {</pre>
        if (!visited[i]) {
          bridge_util(adj, i, visited, disc, low,
              parent);
25
```

3.4 Dijkstra

```
void dijkstra(ll n, vector<vector<pair<ll, ll>>> &
        adj, vector<ll> &dis) {
2
     priority_queue<pair<11, 11>, vector<pair<11, 11</pre>
          >>, greater<pair<11, 11>>> pq;
     for (int i = 0; i < n; i++) {
     dis[i] = INF;
6
     dis[0] = 0;
     pg.push({0, 0});
     while (!pq.empty()) {
       auto p = pq.top();
       pq.pop();
       11 u = p.second;
       if (dis[u] != p.first) {
         continue;
       for (auto x : adj[u]) {
         11 v = x.first, w = x.second;
         if (dis[v] > dis[u] + w) {
           dis[v] = dis[u] + w;
           pq.push({dis[v], v});
```

```
21 }
22 }
23 }
```

3.5 Floyd Warshall

```
void floyd_warshall(vector<vector<ll>>> &dis, ll n)
      for (11 i = 0; i < n; i++) {
        for (11 j = 0; j < n; j++) {
4
          dis[i][j] = (i == j ? 0 : INF);
      for (11 k = 0; k < n; k++) {
        for (11 i = 0; i < n; i++) {
          for (11 j = 0; j < n; j++) {
            if (dis[i][k] < INF && dis[k][j] < INF) {</pre>
11
               dis[i][j] = min(dis[i][j], dis[i][k] +
                   dis[k][j]);
        }
      for (11 i = 0; i < n; i++) {
        for (11 j = 0; j < n; j++) {
18
          for (11 k = 0; k < n; k++) {
19
            if (dis[k][k] < 0 && dis[i][k] < INF && dis</pre>
                 [k][j] < INF) {
               dis[i][j] = -INF;
21
2.2.
23
2.4
25
```

3.6 Hierholzer

```
void print_circuit(vector<vector<ll>>> &adj) {
      map<11, 11> edge_count;
      for (ll i = 0; i < adj.size(); i++) {</pre>
        edge_count[i] = adj[i].size();
      if (!adj.size()) {
        return;
      stack<ll> curr_path;
      vector<11> circuit;
      curr_path.push(0);
      11 curr_v = 0;
      while (!curr_path.empty()) {
        if (edge_count[curr_v]) {
          curr path.push(curr v);
          11 next_v = adj[curr_v].back();
          edge_count[curr_v]--;
          adj[curr_v].pop_back();
          curr_v = next_v;
        } else {
          circuit.push_back(curr_v);
          curr_v = curr_path.top();
          curr_path.pop();
25
      for (ll i = circuit.size() - 1; i >= 0; i--) {
        cout << circuit[i] << ' ';
```

```
3.7 Is Bipartite
 1 bool is_bipartite(vector<11> &col, vector<vector<11</pre>
         >> &adj, 11 n) {
      queue<pair<11, 11>> q;
      for (11 i = 0; i < n; i++) {
        if (col[i] == -1) {
          q.push({i, 0});
          col[i] = 0;
          while (!q.empty()) {
            pair<11, 11> p = q.front();
            q.pop();
            11 v = p.first, c = p.second;
            for (ll j : adj[v]) {
12
              if (col[i] == c) {
13
                return false;
14
15
              if (col[j] == -1) {
16
                col[j] = (c ? 0 : 1);
17
                q.push({j, col[j]});
18
19
20
21
      return true;
```

3.8 Is Cyclic

24 }

```
bool is cyclic util(int u, vector<vector<int>> &adi
         , vector<bool> &vis, vector<bool> &rec) {
      vis[u] = true;
      rec[u] = true;
      for(auto v : adj[u]) {
        if (!vis[v] && is_cyclic_util(v, adj, vis, rec)
            ) {
          return true;
        } else if (rec[v]) {
          return true;
11
      rec[u] = false;
12
      return false;
13 }
14 bool is_cyclic(int n, vector<vector<int>> &adj) {
15
      vector<bool> vis(n, false), rec(n, false);
16
      for (int i = 0; i < n; i++) {</pre>
17
        if (!vis[i] && is_cyclic_util(i, adj, vis, rec)
            ) {
18
          return true;
19
20
21
      return false;
22
```

3.9 Kahn

```
void kahn(vector<vector<1l>>> &adj) {
    11 n = adj.size();
```

```
vector<ll> in_degree(n, 0);
      for (11 u = 0; u < n; u++) {
        for (ll v: adj[u]) {
 6
          in_degree[v]++;
 8
      queue<11> q;
      for (11 i = 0; i < n; i++) {
        if (in_degree[i] == 0) {
          q.push(i);
      11 cnt = 0;
      vector<11> top_order;
      while (!q.empty()) {
      11 u = q.front();
19
       q.pop();
        top_order.push_back(u);
        for (11 v : adj[u]) {
         if (--in_degree[v] == 0) {
            q.push(v);
        cnt++;
      if (cnt != n) {
       cout << -1 << '\n';
30
        return;
      for (11 i = 0; i < (11) top_order.size(); i++) {</pre>
33
        cout << top_order[i] << ' ';
34
      cout << '\n';
36
```

3.10 Maximum Bipartite Matching

```
bool bpm(ll n, ll m, vector<vector<bool>> &bpGraph,
          11 u, vector<bool> &seen, vector<11> &matchR)
      for (11 v = 0; v < m; v++) {
        if (bpGraph[u][v] && !seen[v]) {
          seen[v] = true;
5
          if (matchR[v] < 0 || bpm(n, m, bpGraph,</pre>
               matchR[v], seen, matchR)) {
            matchR[v] = u;
            return true;
 8
        }
      return false:
    11 maxBPM(11 n, 11 m, vector<vector<bool>> &bpGraph
      vector<11> matchR(m, -1);
      11 \text{ result} = 0;
      for (11 u = 0; u < n; u++) {
        vector<bool> seen(m, false);
18
        if (bpm(n, m, bpGraph, u, seen, matchR)) {
          result++;
      return result;
```

3.11 Max Flow

```
1 bool bfs(ll n, vector<vector<ll>>> &r_graph, ll s,
         11 t, vector<11> &parent) {
      vector<bool> visited(n, false);
      queue<11> q;
      q.push(s);
      visited[s] = true;
      parent[s] = -1;
      while (!q.empty()) {
        11 u = q.front();
        q.pop();
        for (11 v = 0; v < n; v++) {
          if (!visited[v] && r_graph[u][v] > 0) {
            if (v == t) {
              parent[v] = u;
               return true;
            q.push(v);
            parent[v] = u;
            visited[v] = true;
120
21
      return false:
23
24
    11 fordFulkerson(ll n, vector<vector<ll>>> graph, ll
          s, 11 t) {
      11 u. v:
      vector<vector<11>> r graph;
27
      for (u = 0; u < n; u++) {
28
        for (v = 0; v < n; v++) {
29
           r_{graph[u][v]} = graph[u][v];
      vector<11> parent;
      11 \text{ max\_flow} = 0;
      while (bfs(n, r_graph, s, t, parent)) {
        11 path_flow = INF;
        for (v = t; v != s; v = parent[v]) {
          u = parent[v];
          path_flow = min(path_flow, r_graph[u][v]);
        for (v = t; v != s; v = parent[v]) {
          u = parent[v];
          r_graph[u][v] -= path_flow;
           r_graph[v][u] += path_flow;
45
        max_flow += path_flow;
      return max flow;
48 }
```

3.12 Prim Mst

```
11 u = pq.top().second;
        pq.pop();
11
        if (in_mst[u]) {
          continue;
13
14
        in_mst[u] = true;
15
        for (auto p : adj[u]) {
16
         11 v = p.first, w = p.second;
17
          if (in_mst[v] == false && w < key[v]) {</pre>
18
            key[v] = w;
19
            pg.push(make_pair(key[v], v));
20
            parent[v] = u;
21
22
        }
23
24
      return parent;
25 }
```

3.13 Strongly Connected Component

```
void dfs(ll u, vector<vector<ll>> &adj, vector<bool</pre>
         > &visited) {
      visited[u] = true;
      cout << u + 1 << ' ';
      for (ll v : adj[u]) {
        if (!visited[v]) {
          dfs(v, adj, visited);
 8
      }
 9
10 vector<vector<ll>> get_transpose(11 n, vector<
         vector<ll>> &adj) {
      vector<vector<ll>> res(n);
12
      for (11 u = 0; u < n; u++) {
13
        for (11 v : adj[u]) {
14
          res[v].push_back(u);
15
16
17
      return res;
18 }
    void fill_order(ll u, vector<vector<ll>>> &adj,
         vector<bool> &visited, stack<ll> &stk) {
      visited[u] = true;
      for(auto v : adj[u]) {
        if(!visited[v]) {
23
           fill_order(v, adj, visited, stk);
24
25
26
      stk.push(u);
27
28 void get_scc(ll n, vector<vector<ll>>> &adj) {
      stack<11> stk:
      vector<bool> visited(n, false);
      for (11 i = 0; i < n; i++) {
        if (!visited[i]) {
          fill_order(i, adj, visited, stk);
34
36
      vector<vector<11>>> transpose = get_transpose(n,
37
      for (ll i = 0; i < n; i++) {</pre>
38
       visited[i] = false;
39
40
      while (!stk.empty()) {
41
        11 u = stk.top();
42
        stk.pop();
43
        if (!visited[u]) {
```

3.14 Topological Sort

```
void dfs(ll v) {
      visited[v] = true;
      for (11 u : adj[v]) {
        if (!visited[u]) {
 5
          dfs(u);
 6
 8
      ans.push_back(v);
 9
    void topological_sort() {
      visited.assign(n, false);
      ans.clear();
      for (11 i = 0; i < n; ++i) {</pre>
       if (!visited[i]) {
          dfs(i);
16
      reverse(ans.begin(), ans.end());
19
```

4 Number Theory

4.1 Extended Euclidean

```
1  ll gcd_extended(ll a, ll b, ll &x, ll &y) {
2    if (b == 0) {
3         x = 1;
4         y = 0;
5         return a;
6    }
7    ll xl, yl, g = gcd_extended(b, a % b, xl, yl);
8    x = yl;
9    y = xl - (a / b) * yl;
10    return g;
11 }
```

4.2 Find All Solutions

```
1 bool find_any_solution(ll a, ll b, ll c, ll &x0, ll
          &v0, 11 &g) {
      q = qcd_extended(abs(a), abs(b), x0, y0);
      if (c % q) {
 4
        return false;
      x0 \star = c / q;
      y0 *= c / g;
8
      if (a < 0) {
9
        x0 = -x0;
10
      if (b < 0) {
12
        y0 = -y0;
      return true;
```

```
16 void shift_solution(11 & x, 11 & y, 11 a, 11 b, 11
      x += cnt * b;
      y -= cnt * a;
19 1
20 11 find_all_solutions(11 a, 11 b, 11 c, 11 minx, 11
          maxx, 11 miny, 11 maxy) {
      11 x, y, g;
      if (!find_any_solution(a, b, c, x, y, g)) {
        return 0;
24
      a /= g;
      b /= q;
      11 \text{ sign}_a = a > 0 ? +1 : -1;
      11 \text{ sign } b = b > 0 ? +1 : -1;
      shift_solution(x, y, a, b, (minx - x) / b);
      if (x < minx) {
        shift_solution(x, y, a, b, sign_b);
      if (x > maxx) {
34
        return 0;
      shift_solution(x, y, a, b, (maxx - x) / b);
38
      if (x > maxx) {
39
        shift_solution(x, y, a, b, -sign_b);
40
41
      11 \text{ rx1} = x;
      shift_solution(x, y, a, b, -(miny - y) / a);
43
      if (y < miny) {
        shift_solution(x, y, a, b, -sign_a);
      if (y > maxy) {
        return 0;
48
49
      11 1x2 = x;
      shift_solution(x, y, a, b, -(maxy - y) / a);
      if (y > maxy) {
52
       shift_solution(x, y, a, b, sign_a);
54
      11 \text{ rx2} = x;
      if (1x2 > rx2) {
        swap(1x2, rx2);
58
      11 1x = max(1x1, 1x2), rx = min(rx1, rx2);
      if (1x > rx) {
60
        return 0;
61
62
      return (rx - 1x) / abs(b) + 1;
```

4.3 Linear Sieve

4.4 Miller Rabin

```
bool check composite(u64 n, u64 a, u64 d, 11 s) {
      u64 x = binpower(a, d, n):
      if (x == 1 | | x == n - 1) {
       return false;
      for (11 r = 1; r < s; r++) {
       x = (u128) x * x % n;
       if (x == n - 1) {
         return false;
     return true;
13
14 bool miller rabin(u64 n) {
    if (n < 2) {
      return false;
17
     11 r = 0;
     u64 d = n - 1;
      while ((d & 1) == 0) {
       d >>= 1;
      for (11 a : {2, 3, 5, 7, 11, 13, 17, 19, 23, 29,
         31, 37}) {
        if (n == a) {
26
         return true;
27
       if (check_composite(n, a, d, r)) {
          return false;
32
      return true;
```

4.5 Modulo Inverse

```
1  ll mod_inv(ll a, ll m) {
2    if (m == 1) {
3        return 0;
4    }
5    ll m0 = m, x = 1, y = 0;
6    while (a > 1) {
7        ll q = a / m, t = m;
8        m = a % m;
9        a = t;
10        t = y;
11        y = x - q * y;
12        x = t;
13    }
14    if (x < 0) {
15        x += m0;
16    }
17    return x;
18 }</pre>
```

4.6 Pollard Rho Brent

```
11 mult(11 a, 11 b, 11 mod) {
 2
     return ( int128 t) a * b % mod;
4
   ll f(ll x, ll c, ll mod) {
5
      return (mult(x, x, mod) + c) % mod;
    11 pollard rho brent(11 n, 11 x0 = 2, 11 c = 1) {
     11 \times = x0, q = 1, q = 1, xs, y, m = 128, 1 = 1;
      while (g == 1) {
       v = x;
        for (11 i = 1; i < 1; i++) {
          x = f(x, c, n);
14
        11 k = 0;
15
        while (k < 1 \&\& q == 1) {
         xs = x;
         for (ll i = 0; i < m && i < l - k; i++) {
          x = f(x, c, n);
           q = mult(q, abs(y - x), n);
          g = \underline{gcd}(q, n);
          k += m;
        1 *= 2;
      if (q == n) {
        do {
        xs = f(xs, c, n);
          g = \underline{gcd}(abs(xs - y), n);
        } while (g == 1);
      return q;
```

4.7 Range Sieve

```
vector<bool> range_sieve(ll l, ll r) {
     11 n = sart(r);
     vector<bool> is prime(n + 1, true);
     vector<ll> prime;
     is_prime[0] = is_prime[1] = false;
      prime.push back(2);
      for (11 i = 4; i <= n; i += 2) {
      is prime[i] = false;
9
10
     for (11 i = 3; i <= n; i += 2) {
      if (is_prime[i]) {
         prime.push back(i);
          for (11 j = i * i; j <= n; j += i) {
           is prime[j] = false;
18
      vector<bool> result(r - 1 + 1, true);
19
      for (ll i : prime) {
       for (11 j = max(i * i, (1 + i - 1) / i * i); j
            <= r; j += i) {
          result[j - 1] = false;
22
     if (1 == 1) {
      result[0] = false;
      return result;
28
```

4.8 Segmented Sieve

```
1 vector<11> segmented sieve(11 n) {
      const 11 S = 10000;
      11 nsqrt = sqrt(n);
     vector<char> is_prime(nsqrt + 1, true);
     vector<ll> prime;
      is prime[0] = is prime[1] = false;
      prime.push_back(2);
      for (11 i = 4; i <= nsqrt; i += 2) {</pre>
       is prime[i] = false;
      for (11 i = 3; i <= nsgrt; i += 2) {</pre>
      if (is prime[i]) {
         prime.push_back(i);
          for (ll j = i * i; j <= nsqrt; j += i) {
           is_prime[j] = false;
       }
      vector<ll> result;
      vector<char> block(S);
      for (11 k = 0; k * S \le n; k++) {
       fill(block.begin(), block.end(), true);
        for (ll p : prime) {
         for (11 j = max((k * S + p - 1) / p, p) * p -
24
             k * S; j < S; j += p) {
           block[j] = false;
         }
        if (k == 0) {
         block[0] = block[1] = false;
        for (11 i = 0; i < S && k * S + i <= n; i++) {
        if (block[i]) {
           result.push_back(k * S + i);
34
      return result;
```

4.9 Tonelli Shanks

```
1  11 legendre(ll a, ll p) {
     return bin_pow_mod(a, (p - 1) / 2, p);
   11 tonelli_shanks(ll n, ll p) {
     if (legendre(n, p) == p - 1) {
        return -1;
      if (p % 4 == 3) {
       return bin_pow_mod(n, (p + 1) / 4, p);
     11 Q = p - 1, S = 0;
      while (0 \% 2 == 0) {
       Q /= 2;
        S++;
      11 z = 2:
      for (; z < p; z++) {</pre>
       if (legendre(z, p) == p - 1) {
          break;
20
```

```
22
       11 M = S, c = bin_pow_mod(z, Q, p), t =
                                                                            if (t2 % p == 1) {
                                                                                                                                          t = t * c % p;
            bin_pow_mod(n, Q, p), R = bin_pow_mod(n, (Q + 1) / 2, p);
                                                                                                                                  38
                                                                                                                                          R = R * b % p;
                                                                              break;
                                                                31
32
33
                                                                                                                                 39
       while (t % p != 1) {
  if (t % p == 0) {
                                                                                                                                 40
23
24
25
26
27
28
                                                                            t2 = t2 * t2 % p;
                                                                                                                                        return R;
                                                                                                                                  41 }
           return 0;
                                                                34
                                                                          11 b = bin_pow_mod(c, bin_pow_mod(2, M - i - 1,
                                                                                p), p);
                                                                35
         11 i = 1, t2 = t * t % p;
                                                                          M = i;
         for (; i < M; i++) {</pre>
                                                                36
                                                                          c = b * b % p;
```

UPLB Eliens 7

f(n) = O(g(n))	iff \exists positive c, n_0 such that	n n n n n n n n n n n n n n n n n n n				
	$0 \le f(n) \le cg(n) \ \forall n \ge n_0.$	$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}, \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}, \sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$				
$f(n) = \Omega(g(n))$	iff \exists positive c, n_0 such that $f(n) \ge cg(n) \ge 0 \ \forall n \ge n_0$.	In general:				
$f(n) = \Theta(g(n))$	iff $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.	$\sum_{i=1}^{n} i^{m} = \frac{1}{m+1} \left[(n+1)^{m+1} - 1 - \sum_{i=1}^{n} \left((i+1)^{m+1} - i^{m+1} - (m+1)i^{m} \right) \right]$				
f(n) = o(g(n))	iff $\lim_{n\to\infty} f(n)/g(n) = 0$.	$\sum_{i=1}^{n-1} i^m = \frac{1}{m+1} \sum_{k=0}^m \binom{m+1}{k} B_k n^{m+1-k}.$				
$\lim_{n \to \infty} a_n = a$	iff $\forall \epsilon > 0$, $\exists n_0$ such that $ a_n - a < \epsilon$, $\forall n \ge n_0$.	Geometric series:				
$\sup S$	least $b \in \mathbb{R}$ such that $b \ge s$, $\forall s \in S$.	$\sum_{i=0}^{n} c^{i} = \frac{c^{n+1} - 1}{c - 1}, c \neq 1, \sum_{i=0}^{\infty} c^{i} = \frac{1}{1 - c}, \sum_{i=1}^{\infty} c^{i} = \frac{c}{1 - c}, c < 1,$				
$\inf S$	greatest $b \in \mathbb{R}$ such that $b \le s$, $\forall s \in S$.	$\sum_{i=0}^{n} ic^{i} = \frac{nc^{n+2} - (n+1)c^{n+1} + c}{(c-1)^{2}}, c \neq 1, \sum_{i=0}^{\infty} ic^{i} = \frac{c}{(1-c)^{2}}, c < 1.$				
$ \liminf_{n \to \infty} a_n $	$\lim_{n \to \infty} \inf \{ a_i \mid i \ge n, i \in \mathbb{N} \}.$	Harmonic series: $H_n = \sum_{i=1}^{n} \frac{1}{i}, \qquad \sum_{i=1}^{n} iH_i = \frac{n(n+1)}{2}H_n - \frac{n(n-1)}{4}.$				
$\limsup_{n \to \infty} a_n$	$\lim_{n \to \infty} \sup \{ a_i \mid i \ge n, i \in \mathbb{N} \}.$	i=1 $i=1$				
$\binom{n}{k}$	Combinations: Size k subsets of a size n set.	$\sum_{i=1}^{n} H_i = (n+1)H_n - n, \sum_{i=1}^{n} {i \choose m} H_i = {n+1 \choose m+1} \left(H_{n+1} - \frac{1}{m+1} \right).$				
$\begin{bmatrix} n \\ k \end{bmatrix}$	Stirling numbers (1st kind): Arrangements of an n element set into k cycles.	1. $\binom{n}{k} = \frac{n!}{(n-k)!k!}$, 2. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$, 3. $\binom{n}{k} = \binom{n}{n-k}$,				
$\left\{ egin{array}{c} n \\ k \end{array} \right\}$	Stirling numbers (2nd kind): Partitions of an n element set into k non-empty sets.	$4. \binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}, \qquad \qquad 5. \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \\ 6. \binom{n}{m} \binom{m}{k} = \binom{n}{k} \binom{n-k}{m-k}, \qquad \qquad 7. \sum_{k=0}^{n} \binom{r+k}{k} = \binom{r+n+1}{n},$				
$\left\langle {n\atop k}\right\rangle$	1st order Eulerian numbers: Permutations $\pi_1\pi_2\pi_n$ on $\{1,2,,n\}$ with k ascents.	$8. \sum_{k=0}^{n} \binom{k}{m} = \binom{n+1}{m+1}, \qquad 9. \sum_{k=0}^{n} \binom{r}{k} \binom{s}{n-k} = \binom{r+s}{n},$				
$\left\langle\!\left\langle {n\atop k}\right\rangle\!\right\rangle$	2nd order Eulerian numbers.	10. $\binom{n}{k} = (-1)^k \binom{k-n-1}{k},$ 11. $\binom{n}{1} = \binom{n}{n} = 1,$				
C_n	Catalan Numbers: Binary trees with $n+1$ vertices.	12. $\binom{n}{2} = 2^{n-1} - 1,$ 13. $\binom{n}{k} = k \binom{n-1}{k} + \binom{n-1}{k-1},$				
		10. $\begin{bmatrix} n \\ n \end{bmatrix} = 1,$ 17. $\begin{bmatrix} n \\ k \end{bmatrix} \ge \begin{Bmatrix} n \\ k \end{Bmatrix},$				
$22. \left\langle {n \atop 0} \right\rangle = \left\langle {n \atop n-1} \right\rangle$	$\begin{pmatrix} n \\ -1 \end{pmatrix} = 1,$ 23. $\begin{pmatrix} n \\ k \end{pmatrix} = \langle n \rangle$	$\binom{n}{n-1-k}$, 24. $\binom{n}{k} = (k+1)\binom{n-1}{k} + (n-k)\binom{n-1}{k-1}$,				
$25. \left\langle {0 \atop k} \right\rangle = \left\{ {1 \atop 0} \right.$	if $k = 0$, otherwise 26. $\begin{cases} r \\ 1 \end{cases}$	$\binom{n}{2} = 2^n - n - 1,$ 27. $\binom{n}{2} = 3^n - (n+1)2^n + \binom{n+1}{2},$				
$25. \ \ \begin{pmatrix} 0 \\ k \end{pmatrix} = \begin{cases} 1 & \text{if } k = 0, \\ 0 & \text{otherwise} \end{cases} $ $26. \ \ \begin{pmatrix} n \\ 1 \end{pmatrix} = 2^n - n - 1, $ $27. \ \ \begin{pmatrix} n \\ 2 \end{pmatrix} = 3^n - (n+1)2^n + \binom{n+1}{2}, $ $28. \ \ x^n = \sum_{k=0}^n \binom{n}{k} \binom{x+k}{n}, $ $29. \ \ \begin{pmatrix} n \\ m \end{pmatrix} = \sum_{k=0}^m \binom{n+1}{k} (m+1-k)^n (-1)^k, $ $30. \ \ m! \begin{Bmatrix} n \\ m \end{Bmatrix} = \sum_{k=0}^n \binom{n}{k} \binom{k}{n-m}, $						
		32. $\left\langle \left\langle n \atop 0 \right\rangle \right\rangle = 1,$ 33. $\left\langle \left\langle n \atop n \right\rangle \right\rangle = 0$ for $n \neq 0,$				
$34. \left\langle \!\! \left\langle \!\! \begin{array}{c} n \\ k \end{array} \!\! \right\rangle = (k + 1)^n $	-1) $\left\langle \left\langle \left$					
$36. \left\{ \begin{array}{c} x \\ x-n \end{array} \right\} = \sum_{k}^{n} \left\{ \begin{array}{c} x \\ x \end{array} \right\}$	$\sum_{k=0}^{n} \left\langle \!\! \left\langle n \right\rangle \!\! \right\rangle \left(x + n - 1 - k \right), $	37. ${n+1 \choose m+1} = \sum_{k} {n \choose k} {k \choose m} = \sum_{k=0}^{n} {k \choose m} (m+1)^{n-k},$				

UPLB Eliens

The Chinese remainder theorem: There exists a number C such that:

$$C \equiv r_1 \bmod m_1$$

: : :

$$C \equiv r_n \bmod m_n$$

if m_i and m_j are relatively prime for $i \neq j$. Euler's function: $\phi(x)$ is the number of positive integers less than x relatively prime to x. If $\prod_{i=1}^{n} p_i^{e_i}$ is the prime factorization of x then

$$\phi(x) = \prod_{i=1}^{n} p_i^{e_i - 1} (p_i - 1).$$

Euler's theorem: If a and b are relatively prime then

$$1 \equiv a^{\phi(b)} \bmod b$$
.

Fermat's theorem:

$$1 \equiv a^{p-1} \bmod p.$$

The Euclidean algorithm: if a > b are integers then

$$gcd(a, b) = gcd(a \mod b, b).$$

If $\prod_{i=1}^{n} p_i^{e_i}$ is the prime factorization of x

$$S(x) = \sum_{d|x} d = \prod_{i=1}^{n} \frac{p_i^{e_i+1} - 1}{p_i - 1}.$$

Perfect Numbers: x is an even perfect number iff $x = 2^{n-1}(2^n - 1)$ and $2^n - 1$ is prime. Wilson's theorem: n is a prime iff $(n-1)! \equiv -1 \mod n$.

$$\mu(i) = \begin{cases} (n-1)! = -1 \mod n. \\ \text{M\"obius inversion:} \\ \mu(i) = \begin{cases} 1 & \text{if } i = 1. \\ 0 & \text{if } i \text{ is not square-free.} \\ (-1)^r & \text{if } i \text{ is the product of} \\ r & \text{distinct primes.} \end{cases}$$
 If

 If

$$G(a) = \sum_{d|a} F(d),$$

$$F(a) = \sum_{d \mid a} \mu(d) G\left(\frac{a}{d}\right).$$

Prime numbers:

$$p_n = n \ln n + n \ln \ln n - n + n \frac{\ln \ln n}{\ln n}$$

$$+O\left(\frac{n}{\ln n}\right),$$

$$\pi(n) = \frac{n}{\ln n} + \frac{n}{(\ln n)^2} + \frac{2!n}{(\ln n)^3} + O\left(\frac{n}{(\ln n)^4}\right).$$

т	$\overline{}$	•	٠			
					m	

Loop An edge connecting a vertex to itself.

Directed Each edge has a direction. SimpleGraph with no loops or multi-edges.

WalkA sequence $v_0e_1v_1\ldots e_\ell v_\ell$. TrailA walk with distinct edges. Pathtrail with distinct

vertices.

ConnectedA graph where there exists a path between any two

vertices.

connected ComponentA maximal subgraph.

TreeA connected acyclic graph. Free tree A tree with no root. DAGDirected acyclic graph. EulerianGraph with a trail visiting each edge exactly once.

Hamiltonian Graph with a cycle visiting each vertex exactly once.

CutA set of edges whose removal increases the number of components.

Cut-setA minimal cut. Cut edge A size 1 cut.

k-Connected A graph connected with the removal of any k-1vertices.

k-Tough $\forall S \subseteq V, S \neq \emptyset$ we have $k \cdot c(G - S) \le |S|$.

A graph where all vertices k-Regular have degree k.

k-Factor Α k-regular spanning subgraph.

Matching A set of edges, no two of which are adjacent.

CliqueA set of vertices, all of which are adjacent.

Ind. set A set of vertices, none of which are adjacent.

Vertex cover A set of vertices which cover all edges.

Planar graph A graph which can be embeded in the plane.

Plane graph An embedding of a planar

$$\sum_{v \in V} \deg(v) = 2m.$$

If G is planar then n - m + f = 2, so

$$f \le 2n - 4, \quad m \le 3n - 6.$$

Any planar graph has a vertex with degree ≤ 5 .

Notation:

E(G)Edge set Vertex set V(G)

c(G)Number of components

G[S]Induced subgraph

deg(v)Degree of v

Maximum degree $\Delta(G)$ $\delta(G)$ Minimum degree Chromatic number

 $\chi(G)$ $\chi_E(G)$ Edge chromatic number G^c Complement graph

 K_n Complete graph

 K_{n_1,n_2} Complete bipartite graph

Ramsev number

Geometry

Projective coordinates: (x, y, z), not all x, y and z zero.

$$(x, y, z) = (cx, cy, cz) \quad \forall c \neq 0.$$

Cartesian Projective (x, y)(x, y, 1)y = mx + b(m, -1, b)

x = c(1,0,-c)Distance formula, L_p and L_{∞}

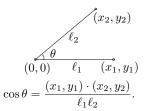
$$\sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2},$$
$$[|x_1 - x_0|^p + |y_1 - y_0|^p]^{1/p},$$

$$\lim_{x \to \infty} \left[|x_1 - x_0|^p + |y_1 - y_0|^p \right]^{1/p}.$$

Area of triangle $(x_0, y_0), (x_1, y_1)$ and (x_2, y_2) :

$$\frac{1}{2} \operatorname{abs} \begin{vmatrix} x_1 - x_0 & y_1 - y_0 \\ x_2 - x_0 & y_2 - y_0 \end{vmatrix}.$$

Angle formed by three points:



Line through two points (x_0, y_0) and (x_1, y_1) :

$$\begin{vmatrix} x & y & 1 \\ x_0 & y_0 & 1 \\ x_1 & y_1 & 1 \end{vmatrix} = 0.$$

Area of circle, volume of sphere:

$$A=\pi r^2, \qquad V=\tfrac{4}{3}\pi r^3.$$

If I have seen farther than others, it is because I have stood on the shoulders of giants.

- Issac Newton

UPLB Eliens

Taylor's series:

$$f(x) = f(a) + (x - a)f'(a) + \frac{(x - a)^2}{2}f''(a) + \dots = \sum_{i=0}^{\infty} \frac{(x - a)^i}{i!}f^{(i)}(a).$$
sions:

Expansions:
$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots = \sum_{i=0}^{\infty} x^i,$$

$$\frac{1}{1-cx} = 1 + x + x^2 + x^3 + x^4 + \cdots = \sum_{i=0}^{\infty} x^i,$$

$$\frac{1}{1-cx} = 1 + cx + c^2x^2 + c^3x^3 + \cdots = \sum_{i=0}^{\infty} c^ix^i,$$

$$\frac{1}{1-x^n} = 1 + x^n + x^{2n} + x^{3n} + \cdots = \sum_{i=0}^{\infty} x^{ni},$$

$$\frac{x}{(1-x)^2} = x + 2x^2 + 3x^3 + 4x^4 + \cdots = \sum_{i=0}^{\infty} ix^i,$$

$$x^k \frac{d^n}{dx^n} \left(\frac{1}{1-x}\right) = x + 2^nx^2 + 3^nx^3 + 4^nx^4 + \cdots = \sum_{i=0}^{\infty} i^nx^i,$$

$$e^x = 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + \cdots = \sum_{i=0}^{\infty} i^i,$$

$$\ln(1+x) = x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \frac{1}{4}x^4 - \cdots = \sum_{i=0}^{\infty} (-1)^{i+1}\frac{x^i}{i},$$

$$\ln \frac{1}{1-x} = x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \frac{1}{4}x^4 + \cdots = \sum_{i=0}^{\infty} (-1)^{i+1}\frac{x^i}{i},$$

$$\sin x = x - \frac{1}{3}x^3 + \frac{1}{5}x^5 - \frac{1}{7}x^7 + \cdots = \sum_{i=0}^{\infty} (-1)^{i}\frac{x^{2i+1}}{(2i+1)!},$$

$$\cos x = 1 - \frac{1}{2}x^2 + \frac{1}{4}x^4 - \frac{1}{6!}x^6 + \cdots = \sum_{i=0}^{\infty} (-1)^{i}\frac{x^{2i+1}}{(2i+1)!},$$

$$1 + x^n = x - \frac{1}{3}x^3 + \frac{1}{5}x^5 - \frac{1}{7}x^7 + \cdots = \sum_{i=0}^{\infty} (-1)^{i}\frac{x^{2i+1}}{(2i+1)!},$$

$$(1+x)^n = 1 + nx + \frac{n(n-1)}{2}x^2 + \cdots = \sum_{i=0}^{\infty} (i)^n x^i,$$

$$\frac{1}{(1-x)^{n+1}} = 1 + (n+1)x + \binom{n+2}{2}x^2 + \cdots = \sum_{i=0}^{\infty} \binom{i}{n}x^i,$$

$$\frac{x}{e^x - 1} = 1 - \frac{1}{2}x + \frac{1}{12}x^2 - \frac{1}{720}x^4 + \cdots = \sum_{i=0}^{\infty} \frac{1}{i} + \binom{2i}{i}x^i,$$

$$\frac{1}{\sqrt{1-4x}} = 1 + x + 2x^2 + 5x^3 + \cdots = \sum_{i=0}^{\infty} \frac{1}{i+1} \binom{2i}{i}x^i,$$

$$\frac{1}{\sqrt{1-4x}} = 1 + x + 2x^2 + 6x^3 + \cdots = \sum_{i=0}^{\infty} \binom{2i+n}{i}x^i,$$

$$\frac{1}{1-x} \ln \frac{1}{1-x} = x + \frac{3}{2}x^2 + \frac{1}{16}x^3 + \frac{25}{12}x^4 + \cdots = \sum_{i=0}^{\infty} \frac{1}{i+1}x^i,$$

$$\frac{1}{1-x} \ln \frac{1}{1-x} = x + \frac{3}{2}x^2 + \frac{1}{16}x^3 + \frac{25}{12}x^4 + \cdots = \sum_{i=0}^{\infty} \frac{1}{i+1}x^i,$$

$$\frac{1}{2} \left(\ln \frac{1}{1-x} \right)^2 = \frac{1}{2}x^2 + \frac{3}{4}x^3 + \frac{11}{12}x^4 + \cdots = \sum_{i=0}^{\infty} \frac{1}{i+1}x^i,$$

$$\frac{x}{1-x-x^2} = x + x^2 + 2x^3 + 3x^4 + \cdots = \sum_{i=0}^{\infty} F_{ni}x^i.$$

Ordinary power series:

$$A(x) = \sum_{i=0}^{\infty} a_i x^i.$$

Exponential power series:

$$A(x) = \sum_{i=0}^{\infty} a_i \frac{x^i}{i!}.$$

Dirichlet power series:

$$A(x) = \sum_{i=1}^{\infty} \frac{a_i}{i^x}.$$

Binomial theorem

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k.$$

$$x^{n} - y^{n} = (x - y) \sum_{k=0}^{n-1} x^{n-1-k} y^{k}.$$

For ordinary power se

$$\alpha A(x) + \beta B(x) = \sum_{i=0}^{\infty} (\alpha a_i + \beta b_i) x^i,$$

$$x^k A(x) = \sum_{i=k}^{\infty} a_{i-k} x^i,$$

$$\frac{A(x) - \sum_{i=0}^{k-1} a_i x^i}{x^k} = \sum_{i=0}^{\infty} a_{i+k} x^i,$$

$$A(cx) = \sum_{i=0}^{\infty} c^i a_i x^i,$$

$$A'(x) = \sum_{i=0}^{\infty} (i+1) a_{i+1} x^i,$$

$$xA'(x) = \sum_{i=1}^{\infty} ia_i x^i,$$

$$\int A(x) dx = \sum_{i=1}^{\infty} \frac{a_{i-1}}{i} x^i,$$

$$\frac{A(x) + A(-x)}{2} = \sum_{i=0}^{\infty} a_{2i} x^{2i},$$

$$\frac{A(x) - A(-x)}{2} = \sum_{i=0}^{\infty} a_{2i+1} x^{2i+1}.$$

Summation: If $b_i = \sum_{i=0}^i a_i$ then

$$B(x) = \frac{1}{1-x}A(x).$$

Convolution:

$$A(x)B(x) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i.$$

God made the natural numbers; all the rest is the work of man. Leopold Kronecker