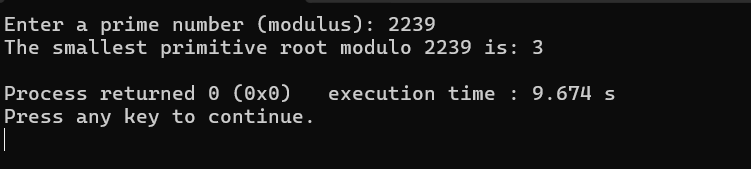
Results：

q=2239, find the original root=3



Q=2239, root=3, n=256

n=256

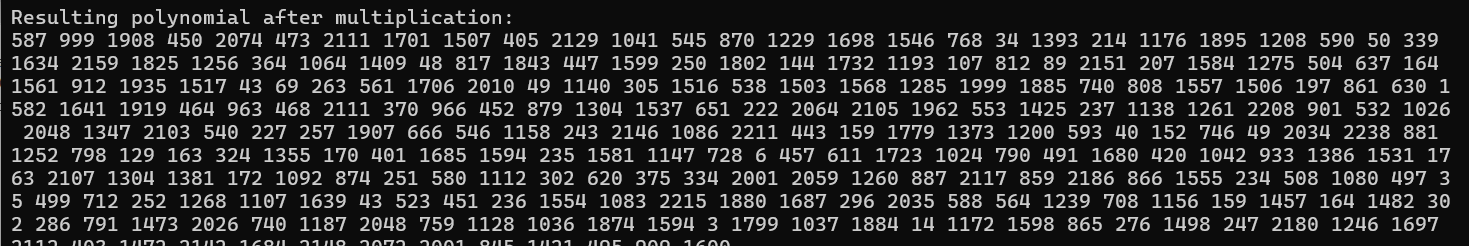
q=2239

A =

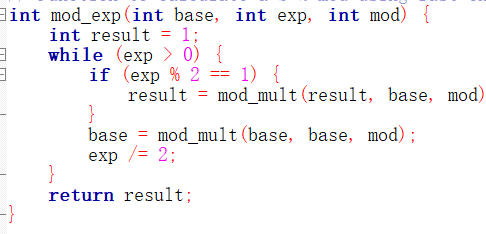
[1038, 1490, 1852, 2012, 1223, 916, 1485, 1215, 1617, 97, 779, 413, 1196, 1374, 992, 967, 1683, 431, 1796, 990, 1893, 1651, 291, 1946, 1340, 1694, 2008, 806, 1278, 279, 885, 567, 688, 1969, 1869, 2204, 359, 2017, 127, 1582, 878, 1456, 1885, 1170, 2137, 1895, 583, 231, 1698, 1270, 214, 2225, 1382, 344, 714, 797, 925, 1972, 227, 956, 612, 1720, 69, 721, 321, 1360, 120, 2049, 730, 10, 302, 788, 2121, 1501, 485, 1896, 1113, 982, 2083, 2202, 419, 2174, 1939, 2207, 504, 931, 739, 1399, 365, 340, 648, 1225, 955, 1613, 723, 643, 127, 1763, 1655, 825, 1627, 1292, 547, 1303, 2117, 141, 165, 1056, 1836, 946, 930, 528, 151, 1810, 637, 1322, 2159, 1515, 1369, 2141, 1016, 2159, 1420, 821, 1598, 588, 1346, 665, 1544, 590, 1939, 1296, 406, 99, 2104, 1056, 1318, 205, 881, 2219, 374, 569, 1605, 637, 948, 1172, 508, 538, 1507, 1318, 540, 914, 2077, 2120, 1809, 43, 1737, 2061, 1960, 17, 357, 895, 1249, 331, 1791, 744, 1903, 2054, 495, 218, 1096, 1394, 826, 952, 320, 1141, 369, 1645, 333, 525, 2034, 744, 201, 1335, 263, 1324, 121, 2158, 1315, 1476, 826, 555, 1326, 485, 264, 980, 2220, 1859, 1521, 684, 809, 1753, 1286, 1686, 1436, 223, 612, 963, 308, 1031, 1762, 1477, 571, 1043, 821, 495, 1516, 1371, 462, 7, 1329, 1416, 1075, 671, 614, 385, 1412, 1511, 1411, 2177, 380, 476, 1345, 799, 282, 2190, 1970, 1952, 166, 842, 1005, 2161, 119, 796, 315, 43, 1957, 1306, 1475, 209, 844, 1212, 947, 721, 920, 1594]

B =

[1844, 1460, 71, 98, 448, 517, 667, 121, 1172, 1330, 471, 1810, 1776, 695, 894, 1297, 1383, 483, 1297, 1959, 2177, 126, 1323, 2215, 1718, 1267, 1353, 153, 1294, 1448, 932, 1652, 354, 525, 165, 1192, 1193, 1368, 1794, 1077, 1484, 747, 704, 102, 178, 9, 1265, 1717, 1265, 1438, 526, 918, 993, 607, 537, 1783, 1434, 1786, 678, 335, 1829, 1708, 88, 994, 1870, 203, 1212, 353, 314, 2044, 186, 1771, 2238, 1748, 567, 1316, 11, 695, 1075, 1627, 1890, 1538, 1455, 152, 1244, 691, 1013, 1783, 1883, 2198, 1960, 280, 1425, 1082, 1071, 1939, 212, 179, 1391, 32, 803, 713, 1958, 934, 1140, 976, 712, 757, 135, 1146, 1972, 646, 240, 1149, 1062, 496, 2124, 1242, 1933, 1603, 1334, 327, 830, 1482, 1123, 86, 2124, 2173, 1109, 29, 37, 1426, 1989, 1493, 854, 766, 812, 709, 124, 1000, 301, 1059, 317, 1913, 11, 62, 809, 1609, 176, 344, 701, 2124, 1822, 1998, 2077, 286, 1000, 307, 527, 647, 1041, 121, 2214, 1990, 1300, 951, 1278, 1352, 1983, 1272, 1983, 917, 532, 841, 594, 1508, 2056, 86, 1814, 1391, 1114, 1462, 1579, 360, 1755, 1279, 832, 1119, 1886, 1793, 842, 1116, 1560, 938, 179, 152, 342, 1109, 878, 5, 1425, 1420, 795, 1100, 454, 437, 778, 1201, 1777, 81, 918, 2221, 224, 280, 1691, 895, 737, 683, 2028, 425, 1643, 1892, 1936, 1170, 414, 882, 2235, 2034, 240, 1804, 1058, 883, 76, 2085, 301, 1520, 1525, 480, 1537, 414, 744, 354, 1996, 608, 2025, 740, 1687, 2063, 1812, 1458, 1390, 614, 19, 1694, 1511, 1124]

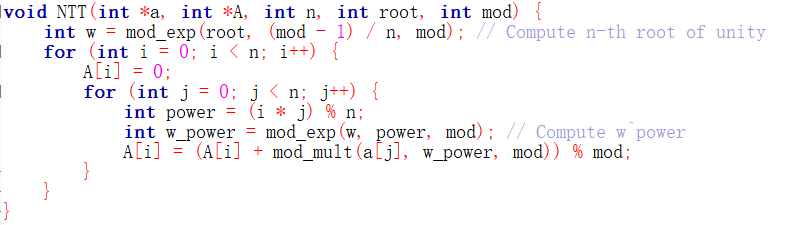


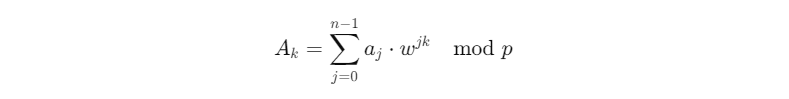
Description:



The "binary exponentiation" (i.e., fast exponentiation algorithm) reduces the time complexity from O(exp) to O(log(exp))

NTT:

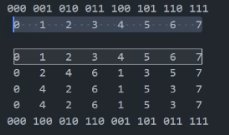




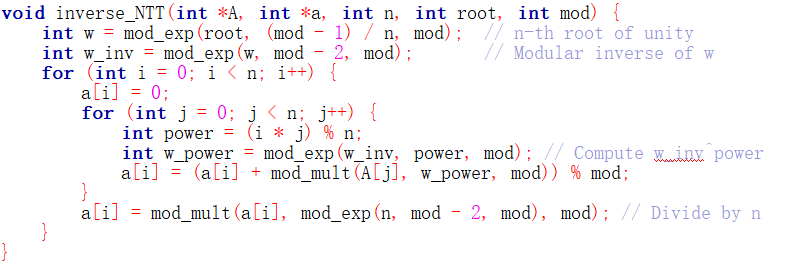
Where w is the nth root of unity (i.e. primitive root), and k = 0, 1, ..., n - 1.

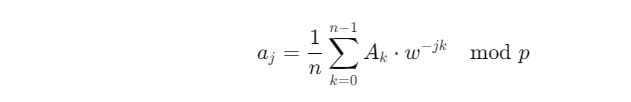
Butterfly:

After the butterfly transformation, it is equivalent to the flipping of the original binary form.



Inverse NTT





Among them, is the modular inverse of w, and needs to be divided by n, which is achieved by multiplying by the modular inverse of n.