#include <stdio.h>

#include <stdbool.h>

// Check if a polynomial is irreducible in GF(2)

bool is\_irreducible(int poly, int m) {

int x = 2; // x in binary (10)

int mod = (1 << m) | 1; // Generate a polynomial of degree m

for (int i = 1; i < (1 << m) - 1; i++) {

x = (x << 1) ^ ((x & (1 << (m - 1))) ? poly : 0);

if (x == 2) return false; // If we loop back to x, it's reducible

}

return true;

}

// Find the first irreducible polynomial of degree m

int find\_irreducible\_polynomial(int m) {

for (int poly = (1 << m) | 1; poly < (1 << (m + 1)); poly += 2) {

if (is\_irreducible(poly, m)) {

return poly;

}

}

return -1;

}

int main() {

int m;

printf("Enter m for GF(2^m): ");

scanf("%d", &m);

int irreducible\_poly = find\_irreducible\_polynomial(m);

if (irreducible\_poly != -1) {

printf("Irreducible monic polynomial for GF(2^%d): x^%d", m, m);

for (int i = m - 1; i >= 0; i--) {

if (irreducible\_poly & (1 << i)) {

printf(" + x^%d", i);

}

}

printf("\n");

} else {

printf("No irreducible polynomial found!\n");

}

return 0;

}