Повернути GF(1), GF(2), .. GF(2n)

*ai* степенева форма

*n = (ai) mod (g(q))* де *g(q)* нерозкладний поліном степеню з таблиці нерозкладних поліномів

p = an

*C = {p1, p2, ..,pq}* де *C* циклотомічний клас

числа

*b1, b2, .., bq = ap1, ap2, .., apq*

*m(x) = (1-b1)(1-b2)..(1-bq)*

де *m(x)* мінімальний зворотній поліном

зберегти an, m(x) та n до GF(i)

Початок

Ввести ступень поля q

Помилка

q ≤ 2

Цикл i=1, .. , 2q