41 Разделить подстановку

Задача. Трент выполняет шифрование слов в алфавите $A = \{0, 1, \ldots, m-1\}$, m — нечетное, с помощью секретной подстановки f: символ открытого текста x при шифровании меняется на символ шифртекста $f(x)$. Трент хочет разделить подстановку f между Алисой и Бобом. Для этого Трент находит подстановки f_1 и f_2, также действующие на A, такие, что

$$f(x) = (f_1(x) + f_2(x)) \bmod m.$$

Подстановку f_1 Трент передает Алисе, а подстановку f_2 — Бобу. Помогите Тренту выполнить разделение. Докажите, что при четном m разделение невозможно.

Решение. Преобразование $x \mapsto ax \bmod m$ является биекцией на A тогда и только тогда, когда числа a и m взаимно просты. Биективны, в частности, преобразования $g(x) = x$, $g_1(x) = 2x \bmod m$, $g_2(x) = (m-1)x \bmod m$. Для них выполняется

$$g(x) = (g_1(x) + g_2(x)) \bmod m.$$

Перейти от g к f можно цепочкой инверсий. Применяя те же инверсии к g_1 и g_2, получаем подстановки f_1 и f_2, которые дают искомое представление.

Если $f(x) = (f_1(x) + f_2(x)) \bmod m$, то

$$\sum x = \sum f(x) \equiv \sum f_1(x) + \sum f_2(x) = 2 \sum x \pmod m$$

(суммирование по $x \in A$). Это возможно, только если сумма элементов A кратна m, что не так при четном m. □