P004 — Quadratic Residue Graph Collisions

Chuah Jia Herng

February 2026

Problem

For a positive integer n, consider the graph with vertex set $\{0, 1, \ldots, n-1\}$. Two *distinct* vertices $i \neq j$ are linked if and only if $i + j$ is a quadratic residue modulo n.

Let $f(n)$ be the number of such unordered links.

1. Find a closed form for $f(n)$.

2. Let k be the greatest integer such that there exists N with the following property: there exists some $n > N$ for which one can find distinct integers $n_1, \ldots, n_k > N$ satisfying

$$f(n) = f(n_1) = \cdots = f(n_k).$$

Determine k.

Idea

Count links by grouping unordered pairs $\{i, j\}$ according to the residue class $s \equiv i + j \pmod{n}$. For each fixed s, the number of such pairs depends only on the parity of n and (when n is even) on the parity of s.

Summing over those s that are quadratic residues introduces the arithmetic function

$$R(n) = \#\{x^2 \bmod n : x \in \mathbb{Z}\},$$

the number of quadratic residues modulo n, and in the even case also the number of odd quadratic residues.

To study multiplicities of $f(n)$, construct explicit pairs of integers producing the same value and iterate the construction.

Solution

Step 1: Counting pairs with a fixed sum

Fix $s \in \{0, 1, \ldots, n-1\}$ and define

$$N_s = \#\big\{\{i, j\} : 0 \leq i < j \leq n-1,\ i + j \equiv s \pmod{n}\big\}.$$

Case 1: n odd. Since 2 is invertible modulo n, the congruence $i \equiv s - i \pmod{n}$ has exactly one solution. Removing this diagonal solution leaves $n - 1$ ordered solutions with $i \neq j$, corresponding to $(n-1)/2$ unordered pairs. Hence

$$N_s = \frac{n-1}{2} \qquad (\forall s).$$

Case 2: n even. Write $n = 2m$.

- If s is odd, there is no diagonal solution, giving $m = n/2$ unordered pairs.
- If s is even, there are two diagonal solutions, so removing them leaves $2m-2$ ordered solutions with $i \neq j$, giving $(n-2)/2$ unordered pairs.

Step 2: Closed form for $f(n)$

Define
$$R(n) = \#\{x^2 \bmod n : x \in \mathbb{Z}\}.$$

If n is odd, each quadratic residue s contributes $(n-1)/2$ unordered pairs, hence
$$f(n) = \frac{n-1}{2} R(n).$$

If n is even, define $R_{\text{odd}}(n)$ to be the number of odd quadratic residues modulo n. Summing contributions gives
$$f(n) = \frac{n}{2} R_{\text{odd}}(n) + \frac{n-2}{2}\big(R(n) - R_{\text{odd}}(n)\big) = \frac{n-2}{2} R(n) + R_{\text{odd}}(n).$$

Step 3: Infinite collision chains

Claim. If u is odd and $3 \nmid u$, then
$$f(6u) = f(8u).$$

Proof. Using multiplicativity and the values
$$R(2) = 2, \quad R(3) = 2, \quad R(8) = 3, \quad R_{\text{odd}}(2) = 1, \quad R_{\text{odd}}(8) = 1,$$
we obtain
$$R(6u) = 4R(u), \quad R_{\text{odd}}(6u) = R(u),$$
$$R(8u) = 3R(u), \quad R_{\text{odd}}(8u) = R(u).$$
Therefore
$$f(6u) = \frac{6u-2}{2} \cdot 4R(u) + R(u) = 2(6u-1)R(u),$$
$$f(8u) = \frac{8u-2}{2} \cdot 3R(u) + R(u) = 2(6u-1)R(u),$$
proving the claim.

Now define
$$n_t = 6 \cdot 4^t u \qquad (t = 0, 1, 2, \dots).$$
Then
$$n_{t+1} = 8 \cdot 4^t u,$$
and applying the claim to $4^t u$ yields
$$f(n_t) = f(n_{t+1}) \quad \text{for all } t \geq 0.$$

Hence
$$f(n_0) = f(n_1) = f(n_2) = \cdots,$$
with all n_t distinct and unbounded.

Given any N and k, choose u large enough so that $n_0 = 6u > N$. Then $n_0, n_1, \dots, n_k > N$ and all have the same f-value. Thus no greatest k exists.

Remarks

- The formulas reduce the problem to the arithmetic of quadratic residues, governed by CRT and prime-power behavior.
- The collision construction exploits the identities $R(6u) = 4R(u)$ and $R(8u) = 3R(u)$ together with identical odd-residue counts.