The Quadratic Reciprocity Law (6)

Proof of Eisenstein's Lemma (Part 1)

$P = 2N+1$. For $1 \le K \le N$, take $1 \le C_K \le P-1$ s.t.

$$C_K \equiv 2KQ \pmod{P}$$

$(2KQ-C_K)/P$ = (# of lattice points with x-coord $2K$)

M = (sum of $(2KQ - C_K)/P$)

$\equiv$ (sum of C_K) (mod 2)

$\equiv$ (# of K such that C_K is odd) (mod 2)

Put $D_K = C_K$ if C_K is even. Otherwise, $D_K = P-C_K$.

The Quadratic Reciprocity Law (7)

Proof of Eisenstein's Lemma (Part 2)

- $2 \le D_1, \cdots, D_N \le 2N = P-1$ are **distinct** even integers. ($D_I = D_J \Rightarrow C_I \equiv \pm C_J \Rightarrow 2IQ \equiv \pm 2JQ \Rightarrow I \equiv \pm J \Rightarrow I = J$)

$$(\text{prod of } D_K) = 2 \times 4 \times \cdots \times 2N$$

- Since $C_K \equiv 2KQ$,

$$(\text{prod of } C_K) \equiv Q^N \times 2 \times 4 \times \cdots \times 2N$$

$\Rightarrow (-1)^M \equiv Q^N \pmod{P}$.

By **Euler's Criterion,** $(-1)^M = \left(\dfrac{Q}{P}\right)$