Quadratic Reciprocity

Gautham Anne

Family 81

2022

Table of Contents

Lemma 1. Let $p \in \mathbb{Z}$ be a prime. If $a \in U_p$, for all $k \in \mathbb{Z}_p, \exists \epsilon_k, r_k \in \mathbb{Z}_p$ such that $a \cdot k \equiv \epsilon_k \cdot r_k \pmod{p}$, where $\epsilon_k \in \{-1, 1\}$ and $0 \leq r_k < \frac{p}{2}$. Then for each $k \in \{1, 2, ..., \frac{p-1}{2}\}, r_k$ is unique.

Lemma 2. If $a \in \mathbb{Z}_p$:

$$(\frac{p}{q}) = (-1)^{\prod_{k=1}^{\frac{p-1}{2}} \epsilon_k}$$

Gauss's Lemma. For distinct odd primes p, q :

$$(\frac{p}{q}) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{2qk}{p} \rfloor}$$

Table of Contents (Continued)

Lemma 3. For distinct primes p, q, we have in $\mathbb{Z}_2$:

$$\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{2qk}{p} \rfloor \equiv \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{qk}{p} \rfloor$$

Lemma 4. If $\gcd(a, b) = 1$, then:

$$\sum_{x=1}^{\frac{b-1}{2}} \lfloor \frac{ax}{b} \rfloor + \sum_{y=1}^{\frac{a-1}{2}} \lfloor \frac{by}{a} \rfloor = \frac{a-1}{2} \cdot \frac{b-1}{2}$$

Quadratic Reciprocity. Let p, q be distinct odd primes. Then:

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Lemma 1

Suppose p is an odd prime and $a \neq 0 \pmod{p}$.
For each $k \in \{b \in \mathbb{Z} | 1 \leq b \leq \frac{p-1}{2}\}$, define ϵ_k and r_k by $ak \equiv \epsilon_k r_k \pmod{p}$ where $0 < r_k < \frac{p-1}{2}$ and $\epsilon_k = \pm 1$

Claim: $\{r_k \in \mathbb{Z} | 1 \leq k \leq \frac{p-1}{2}\} = \{b \in \mathbb{Z} | 1 \leq b \leq \frac{p-1}{2}\}$
Proof: For the sake of contradiction, assume that $r_i = r_j$ for some $1 \leq i, j \leq \frac{p-1}{2}, i \neq j$. Then $ai \equiv aj$ or $ai \equiv -aj$. $ai \not\equiv -aj$ because $ai \equiv -aj$ directly implies that $i \equiv -j$ as $gcd(a, p) = 1$. However, $i \not\equiv -j$ because $1 \leq i, j \leq \frac{p-1}{2}$.
Therefore, $ai \equiv aj \implies a(i-j) \equiv 0 \implies a \equiv 0$ or $i - j \equiv 0 \implies i \equiv j$.
Since $1 \leq i, j \leq \frac{p-1}{2}$, $-p < \frac{3-p}{2} \leq i - j \leq p - 2 < p$. Therefore, $i - j = 0 \implies i = j$.
We arrive at a contradiction, because we assumed that $i \neq j$. Hence, our claim holds true.

Lemma 2

Claim: $a^{\frac{p-1}{2}} = (-1)^{\prod_{j=1}^{\frac{p-1}{2}} \epsilon_j}$

Proof : $\prod_{j=1}^{\frac{p-1}{2}} aj = a^{\frac{p-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} j$

$\prod_{j=1}^{\frac{p-1}{2}} \epsilon_j r_j = \prod_{j=1}^{\frac{p-1}{2}} \epsilon_j \cdot \prod_{j=1}^{\frac{p-1}{2}} r_j = \prod_{j=1}^{\frac{p-1}{2}} \epsilon_j \cdot \prod_{j=1}^{\frac{p-1}{2}} j$ because using Lemma 1, $\prod_{j=1}^{\frac{p-1}{2}} r_j = \prod_{j=1}^{\frac{p-1}{2}} j$.

Since $\prod_{j=1}^{\frac{p-1}{2}} aj = \prod_{j=1}^{\frac{p-1}{2}} \epsilon_j r_j$,

$a^{\frac{p-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} j = \prod_{j=1}^{\frac{p-1}{2}} \epsilon_j \prod_{j=1}^{\frac{p-1}{2}} j \implies a^{\frac{p-1}{2}} = \prod_{j=1}^{\frac{p-1}{2}} \epsilon_j$

Gauss's Lemma

Claim: For distinct odd primes p, q : $(\frac{p}{q}) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{2qk}{p} \rfloor}$ *Proof* : Using $ak \equiv \epsilon_k r_k$ where $0 < r_k < \frac{p}{2}, 2ak \equiv 2\epsilon_k r_k \pmod{p}$. Then, $2ak = np + 2\epsilon_k r_k \implies \frac{2ak}{p} = n + \frac{2\epsilon_k r_k}{p} \implies \lfloor \frac{2ak}{p} \rfloor = n + \lfloor \frac{2\epsilon_k r_k}{p} \rfloor$. Since $pn = 2ak - 2\epsilon_k r_k = 2(ak - \epsilon_k r_k)$, n must be even (p is an odd prime). Therefore, if $\epsilon_k = 1, \lfloor \frac{2\epsilon_k r_k}{p} \rfloor = 0$ as $0 < r_k < \frac{p}{2}$, so $\lfloor \frac{2ak}{p} \rfloor = n$, which is an even number and if $\epsilon_k = -1, \lfloor \frac{2\epsilon_k r_k}{p} \rfloor = -1$, so $\lfloor \frac{2ak}{p} \rfloor = n - 1$,which is an odd number. Therefore, the parity of $\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{2qk}{p} \rfloor$ will be odd if there is an odd number of $\epsilon_k = -1$ where $1 \leq k \leq \frac{p-1}{2}$. Then by Lemma 2, we conclude:

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{2qk}{p} \rfloor} = (\frac{p}{q}).$$

Lemma 3

By Division Theorem, $qk = \lfloor \frac{qk}{p} \rfloor \cdot p + r_1$ for $r_1 \in \mathbb{Z}$. Then $q(p-k) = \lfloor \frac{qk}{p} \rfloor \cdot p + (p - r_1)$, so:

$$\frac{qk}{p} + \frac{q(p-k)}{p} = \lfloor \frac{qk}{p} \rfloor + \lfloor \frac{q(p-k)}{p} \rfloor + \frac{r_1}{p} + (1 - \frac{r_1}{p}) = a$$

$$\rightarrow \lfloor \frac{qk}{p} \rfloor + \lfloor \frac{q(p-k)}{p} \rfloor = a - 1 \rightarrow \lfloor \frac{qk}{p} \rfloor \equiv \lfloor \frac{q(p-k)}{p} \rfloor (mod 2)$$

Then note:

$$\lfloor \frac{2q(\frac{p-1}{2} - k)}{p} \rfloor = \lfloor \frac{q(p-1-2k)}{p} \rfloor \equiv \lfloor \frac{q(2k+1)}{p} \rfloor$$

$$\lfloor \frac{2qk}{p} \rfloor = \lfloor \frac{q(2k)}{p} \rfloor$$

Lemma 3 (Continued)

Then note that:

$$\sum_{k=0}^{\frac{p-1}{2}} \lfloor \frac{2qk}{p} \rfloor = \sum_{0 \le k \le \frac{p-1}{4}} \lfloor \frac{2qk}{p} \rfloor + \sum_{\frac{p-1}{4} < k \le \frac{p-1}{2}} \lfloor \frac{2qk}{p} \rfloor$$

$$\equiv \sum_{0 \le k \le \frac{p-1}{4}} \lfloor \frac{q(2k)}{p} \rfloor + \sum_{0 \le k < \frac{p-1}{4}} \lfloor \frac{q(2k+1)}{p} \rfloor = \sum_{k=0}^{\frac{p-1}{2}} \lfloor \frac{qk}{p} \rfloor$$

Since $\lfloor \frac{q \cdot 0}{p} \rfloor = 0 = \lfloor \frac{2q \cdot 0}{p} \rfloor$, the above simplifies to:

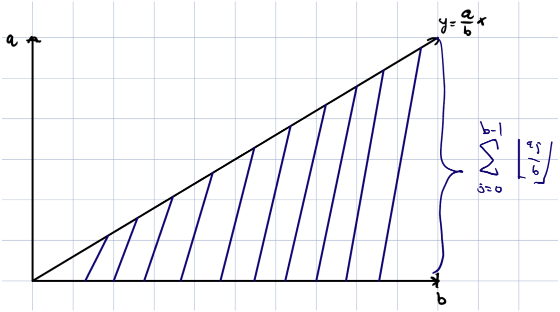
$$\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{2qk}{p} \rfloor \equiv \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{qk}{p} \rfloor$$

As desired.

https://www.overleaf.com/project/62e08a46f4d4e2e250a8d0f2

Lemma 4

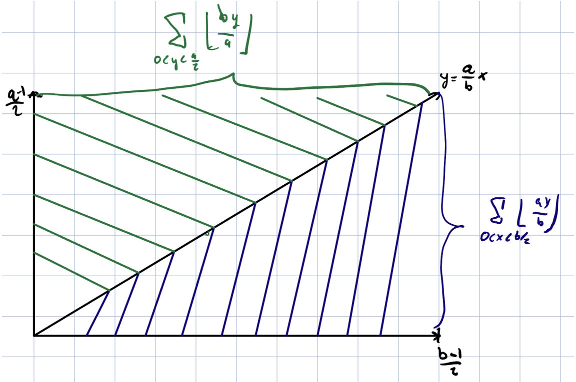
Consider the sum $\sum_{j=0}^{b-1} \lfloor \frac{aj}{b} \rfloor = \frac{(a-1)(b-1)}{2}$. The sum is equal to the number of lattice points inside and on the boundary of the triangle formed by $(0,0), (b,0), (0,a)$.



So, the number of lattice points can be found by finding the area of the triangle, which is $\frac{(a-1)(b-1)}{2}$.

Lemma 4 (Continued)

Now, we consider the summation $\sum_{0<x<\frac{b}{2}} \lfloor \frac{ax}{b} \rfloor + \sum_{0<y<\frac{b}{2}} \lfloor \frac{ay}{b} \rfloor$. From the last slide, we see that this represents:



So, the addition is counting the number of lattice points inside the rectangle, which we find by taking the product $\frac{a-1}{2} \cdot \frac{b-1}{2}$.

Quadratic Reciprocity

By Gauss's Lemma, Lemma 3, and Lemma 4:

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\sum_{k=0}^{\frac{p-1}{2}} \lfloor \frac{2qk}{p} \rfloor + \sum_{k=0}^{\frac{q-1}{2}} \lfloor \frac{2pk}{q} \rfloor}$$

$$= (-1)^{\sum_{k=0}^{\frac{p-1}{2}} \lfloor \frac{qk}{p} \rfloor + \sum_{k=0}^{\frac{q-1}{2}} \lfloor \frac{pk}{q} \rfloor} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

As desired. This concludes our proof of Quadratic Reciprocity and this presentation as a whole.