7. Quadratic reciprocity

7.1 Gauss's Lemma

Lemma 7.1 (Gauss's Lemma). Let $p \geq 3$ be a prime and a be such that $(a,p)=1$. For each k with $1 \leq k \leq \frac{p-1}{2}$, let r_k be the smallest nonnegative residue of ak modulo p. If $\mu = \mu_a$ counts the number of r_k greater than $\frac{p}{2}$, then

$$\left(\frac{a}{p}\right) = (-1)^{\mu}. \tag{7.1}$$

Proof. Since $(a,p)=1$, we have $1 \leq r_k \leq p-1$ for each k. Assume that $x_1,\ldots,x_\mu$ are those $r_k > \frac{p}{2}$ and $y_1,\ldots,y_\nu$ are those $r_k < \frac{p}{2}$. Note that $\mu+\nu = \frac{p-1}{2}$. Also, the x's are pairwise distinct and so are the y's. We further claim that there are no x_i and y_j with $p-x_i = y_j$; otherwise, we have k_i and k_j such that $ak_i + ak_j \equiv 0 \pmod{p}$, or $k_i + k_j \equiv 0 \pmod{p}$, which is impossible since $1 \leq k_i, k_j \leq \frac{p-1}{2}$. Noting that $1 \leq (p-x), y < \frac{p}{2}$, we conclude that the $\frac{p-1}{2}$ integers $(p-x_1),\ldots,(p-x_\mu)$ and $y_1,\ldots,y_\nu$ form a rearrangement of $1,\ldots,\frac{p-1}{2}$. Thus,

$$\begin{aligned} a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= \prod_{k=1}^{(p-1)/2}(ak) \equiv \prod_{k=1}^{(p-1)/2} r_k = \prod_{i=1}^{\mu} x_i \cdot \prod_{j=1}^{\nu} y_j \\ &\equiv (-1)^{\mu}\prod_{i=1}^{\mu}(p-x_i)\cdot\prod_{j=1}^{\nu} y_j = (-1)^{\mu}\left(\frac{p-1}{2}\right)! \pmod{p}. \end{aligned}$$

Since $(\frac{p-1}{2})!$ is coprime to p, we have $a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod{p}$. Finally, (7.1) follows since $\left(\frac{a}{p}\right)$ takes value from $\{\pm 1\}$ by definition and $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ by Theorem 6.6. ∎

For any real number x, let $\lfloor x \rfloor$ denote the largest integer not exceeding x.

Lemma 7.2 With the notation in Lemma 7.1, we have

$$\mu_a \equiv (a-1)\cdot\frac{p^2-1}{8} + \sum_{k=1}^{(p-1)/2}\left\lfloor \frac{ak}{p} \right\rfloor \pmod{2}. \tag{7.2}$$

Proof. Note that each r_k is the remainder of ak divided by p. Thus, $ak = p\cdot\lfloor\frac{ak}{p}\rfloor + r_k$. Now,

recalling that p is an odd prime,

$$\begin{aligned} a\cdot\frac{p^2-1}{8} &= \sum_{k=1}^{(p-1)/2}(ak) = \sum_{k=1}^{(p-1)/2}\left(p\cdot\left\lfloor\frac{ak}{p}\right\rfloor + r_k\right) = p\sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ak}{p}\right\rfloor + \sum_{i=1}^{\mu}x_i + \sum_{j=1}^{\nu}y_j \\ &\equiv \sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ak}{p}\right\rfloor + \left(\mu + \sum_{i=1}^{\mu}(p-x_i)\right) + \sum_{j=1}^{\nu}y_j = \sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ak}{p}\right\rfloor + \mu + \sum_{k=1}^{(p-1)/2}k \\ &= \sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ak}{p}\right\rfloor + \mu + \frac{p^2-1}{8} \pmod 2, \end{aligned}$$

thereby yielding the desired result. ■

7.2 When is 2 a quadratic residue modulo p?

Theorem 7.3 Let $p \geq 3$ be a prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{7.3}$$

In particulae, 2 is a quadratic residue modulo p if $p \equiv \pm 1 \pmod 8$, and a quadratic non-residue modulo p if $p \equiv \pm 3 \pmod 8$.

Proof. Note that for k with $1 \leq k \leq \frac{p-1}{2}$, we have $0 < \frac{2k}{p} < 1$ and thus $\lfloor\frac{2k}{p}\rfloor = 0$. Now, taking $a = 2$ in (7.3) gives $\mu_2 \equiv \frac{p^2-1}{8} \pmod 2$, and it follows from Gauss's Lemma that $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod p$. Hence, (7.3) follows since $\left(\frac{2}{p}\right)$ takes value from $\{-1,1\}$ for odd primes p. Finally, $\frac{p^2-1}{8}$ is even if $p \equiv \pm 1 \pmod 8$, and odd if $p \equiv \pm 3 \pmod 8$. ■

7.3 Guass's law of quadratic reciprocity

We have witnessed from Gauss's Lemma (Lemma 7.1) and Lemma 7.2 that for $p \geq 3$ a prime and a an integer with $(a,p) = 1$,

$$\left(\frac{a}{p}\right) = (-1)^{(a-1)\cdot\frac{p^2-1}{8} + \sum_{k=1}^{(p-1)/2}\lfloor\frac{ak}{p}\rfloor}.$$

Now, we further assume that $q \geq 3$ is a prime such that $q \neq p$. Then $(q-1)\cdot\frac{p^2-1}{8}$ is even for $q-1$ is even and $\frac{p^2-1}{8} = \sum_{k=1}^{(p-1)/2}k$ is an integer. It follows that

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2}\lfloor\frac{kq}{p}\rfloor}.$$

Similarly,

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{(q-1)/2}\lfloor\frac{kp}{q}\rfloor}.$$

It turns out that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{(p-1)/2}\lfloor\frac{kq}{p}\rfloor + \sum_{k=1}^{(q-1)/2}\lfloor\frac{kp}{q}\rfloor}. \tag{7.4}$$

Theorem 7.4 Let $p,q \geq 3$ be primes with $p \neq q$. Then

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor = \frac{(p-1)(q-1)}{4}. \tag{7.5}$$

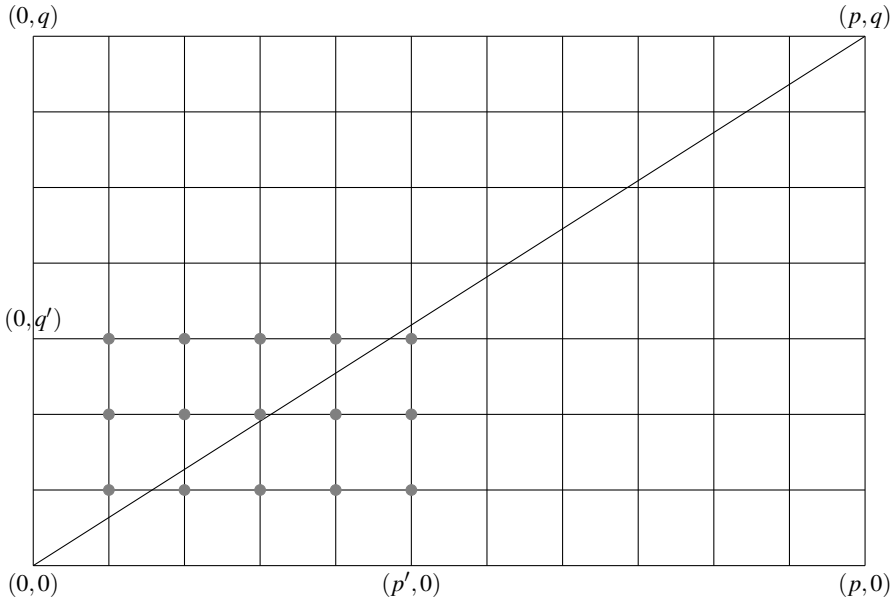

Figure 7.1: Integer lattices and $y = \frac{q}{p}x$

Proof. For convenience, we write $p' = \frac{p-1}{2}$ and $q' = \frac{q-1}{2}$. Consider the line

$$\ell : y = \frac{q}{p}x$$

on the xy-plane. We begin with some observations.

Observation 1. *For any integer $k \geq 1$, $\lfloor \frac{kq}{p} \rfloor$ equals the number of points with integer coordinates, or lattices for short, (k,y) which are below ℓ (with lattices on ℓ included).* For its proof, we note that ℓ touches the vertical line $x = k$ at $(k, \frac{kq}{p})$. Thus, such lattices are those with $1 \leq y \leq \frac{kq}{p}$, and the number of them equals the integer part of $\frac{kq}{p}$, that is $\lfloor \frac{kq}{p} \rfloor$.

Observation 2. *For any integer $k \geq 1$, $\lfloor \frac{kp}{q} \rfloor$ equals the number of lattices (x,k) which are above ℓ (with lattices on ℓ included).* The proof is similar to that for the first observation — we only need to note that ℓ touches the horizontal line $y = k$ at $(\frac{kp}{q}, k)$.

Observation 3. *There is no lattice (x,y) with $1 \leq x \leq p'$ or $1 \leq y \leq q'$ that is on ℓ.* Otherwise, assume that there exists an x_0 with $1 \leq x_0 \leq p'$ such that $(x_0, \frac{q}{p}x_0)$ is a lattice. Then $\frac{q}{p}x_0$ is an integer, which is impossible since $p \nmid q$ for p,q are distinct odd primes and $p \nmid x_0$ for $1 \leq x \leq p' = \frac{p-1}{2}$. Similarly, if we assume that there exists a y_0 with $1 \leq y_0 \leq q'$ such that $(\frac{p}{q}y_0, y_0)$ is a lattice, then $\frac{p}{q}y_0$ is an integer, and it is also impossible. The claim follows by contradiction.

Now, we focus on the set of lattices (x,y) with $1 \leq x \leq p'$ and $y \geq 1$ that are **strictly** below ℓ, denoted by $\mathscr{B}$, and the set of lattices (x,y) with $x \geq 1$ and $1 \leq y \leq q'$ that are **strictly** above ℓ, denoted by $\mathscr{A}$.

By the three observations (especially Observation 3, which allows us to add the strengthening of "**strictly**"), we have

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor = \operatorname{card} \mathscr{A} + \operatorname{card} \mathscr{B}.$$

First, it is apparent that all lattices (x,y) with $1 \le x \le p'$ **and** $1 \le y \le q'$ are in $\mathscr{A} \cup \mathscr{B}$. Now, we show that they are the only lattices in $\mathscr{A} \cup \mathscr{B}$.

(i). For lattices with $x > p'$ and $y > q'$, they are not in $\mathscr{A} \cup \mathscr{B}$ by definition.

(ii). For any lattice with $1 \le x \le p'$ and $y > q'$ (so it is not in $\mathscr{A}$), we compute the slope of the line connecting this lattice and the origin, which is $\frac{y}{x} \ge \frac{q'+1}{p'} = \frac{q+1}{p-1} > \frac{q}{p}$, and thus the lattice is above ℓ, so not in $\mathscr{B}$.

(iii). For any lattice with $x > p'$ and $1 \le y \le q'$ (so it is not in $\mathscr{B}$), we compute the slope of the line connecting this lattice and the origin, which is $\frac{y}{x} \le \frac{q'}{p'+1} = \frac{q-1}{p+1} < \frac{q}{p}$, and thus the lattice is below ℓ, so not in $\mathscr{A}$.

Noting that $\mathscr{A}$ and $\mathscr{B}$ are disjoint, we have $\operatorname{card} \mathscr{A} + \operatorname{card} \mathscr{B} = \operatorname{card} \mathscr{A} \cup \mathscr{B} = p'q'$. Thus,

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor = \operatorname{card} \mathscr{A} + \operatorname{card} \mathscr{B} = p'q' = \frac{(p-1)(q-1)}{4},$$

proving the desired result. ■

Now, we can state Guass's law of quadratic reciprocity.

Theorem 7.5 (Guass's Law of Quadratic Reciprocity). Let $p,q \ge 3$ be primes with $p \ne q$. Then

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}. \tag{7.6}$$

Proof. This is a direct application of (7.4) and (7.5). ■

7.4 When is 3 a quadratic residue modulo p?

Theorem 7.6 Let $p \ge 5$ be a prime. Then 3 is a quadratic residue modulo p if $p \equiv \pm 1 \pmod{12}$, and a quadratic non-residue modulo p if $p \equiv \pm 5 \pmod{12}$.

Proof. By Guass's law of quadratic reciprocity, we have

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}.$$

Further, $\left(\frac{p}{3}\right)$ equals 1 if $p \equiv 1 \pmod 3$ and equals -1 if $p \equiv -1 \pmod 3$. Also, $(-1)^{\frac{p-1}{2}}$ equals 1 if $p \equiv 1 \pmod 4$ and equals -1 if $p \equiv -1 \pmod 4$. The desired result follows by a simple calculation. ■

7.5 An upper bound for the least quadratic non-residue

Definition 7.1 Let $p \ge 3$ be a prime. The *least quadratic non-residue modulo* p, usually denoted by n_p, is the smallest positive integer that is a quadratic non-residue modulo p.

■ **Example 7.1** We have $n_3 = 2$, $n_5 = 2$, $n_7 = 3$, ... ■

R The least quadratic residue is less interesting because 1 is always a quadratic residue modulo any odd prime p.

Recall from Theorem 6.2 that there are $\frac{p-1}{2}$ residues and $\frac{p-1}{2}$ non-residues modulo p among $1,\ldots,p-1$. Therefore, we trivially have $n_p \le \frac{p-1}{2}+1 = \frac{p+1}{2}$. But the upper bound for n_p could be sharper.

Theorem 7.7 Let $p \ge 3$ be a prime. Then

$$n_p < \sqrt{p}+1. \tag{7.7}$$

Proof. Note that $1 < n_p < p$. Let $m = \lfloor \frac{p}{n_p} \rfloor + 1$. Since $\frac{p}{n_p}$ is not an integer, we have $(m-1)n_p < p < mn_p$. Thus, $0 < mn_p - p < n_p$. Since n_p is the least non-residue, we have that all $1,\ldots,n_p-1$ are residues, and so is $mn_p - p$. It follows that

$$1 = \left(\frac{mn_p - p}{p}\right) = \left(\frac{mn_p}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n_p}{p}\right),$$

where Theorem 6.7 is used. Since n_p is a non-residue, we have $\left(\frac{n_p}{p}\right) = -1$, and thus $\left(\frac{m}{p}\right) = -1$ from the above. Thus, m is also a non-residue. It follows that $n_p \le m$. So,

$$p > (m-1)n_p \ge (n_p-1)n_p > (n_p-1)^2,$$

yielding the desired result. ■

R The upper bound for n_p is far sharper than (7.7). The best bound known today is

$$n_p = O_\varepsilon\left(p^{\frac{1}{4\sqrt{e}}+\varepsilon}\right),$$

for all $\varepsilon > 0$. It was proved with recourse to Burgess's estimate of certain character sums and Vinogradov's sieving trick. An excellent exposition of the idea can be found in Terry Tao's blog post:

https://terrytao.wordpress.com/2009/08/18/the-least-quadratic-nonresidue-and-the-square-root-barrier/