Technical Lemma

Let p be an odd prime, $a \in \mathbb{Z}$ be odd and $\gcd(a,p)=1$ then

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

proof: We use Gauss's Lemma and its notation. It is enough to show that

$$n \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \mod 2$$

We first look at $\left\lfloor \frac{ka}{p} \right\rfloor$, we'll need this later.

Let $ka = q_k p + t_k \quad 0 < t_k < p$

(note that $t_k \not\equiv 0$ since both $k, a \not\equiv 0 \mod p$)

Then $\left\lfloor \frac{ka}{p} \right\rfloor = \left\lfloor \frac{q_k p + t_k}{p} \right\rfloor = \left\lfloor q_k + \frac{t_k}{p} \right\rfloor = q_k$

Now to the proof: The idea is to compare

$$\sum_{k=1}^{\frac{p-1}{2}} ka = a \sum_{k=1}^{\frac{p-1}{2}} k \quad \text{and} \quad \sum_{k=1}^{\frac{p-1}{2}} k$$

First $\sum_{k=1}^{\frac{p-1}{2}} k$:

First since $k=1,2,3\ldots\frac{p-1}{2}$, and we are doing ka, we have that the remainders t_k are exactly the remainders $r_1, r_2, \ldots r_m, s_1, s_2 \ldots s_n$ from the proof of Gauss's lemma. From there we know that

$$r_1, r_2 \ldots r_m,\ p-s_1,\ p-s_2,\ \ldots\ p-s_n$$

are exactly $1, 2, \ldots \frac{p-1}{2}$. So

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} (p-s_j)$$

$$= np + \sum_{i=1}^{m} r_i - \sum_{j=1}^{n} s_j$$

Now $\sum_{k=1}^{\frac{p-1}{2}} ka$:

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} (q_k p + t_k)$$

$$= \sum_{k=1}^{\frac{p-1}{2}} q_k p + \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_j$$

$$= p \sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_j$$

$$\sum_{k=1}^{\frac{p-1}{2}} ka = p\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_j$$

Now notice that since a is odd, $a \equiv 1 \bmod 2$
so
$$\sum_{k=1}^{\frac{p-1}{2}} ka = a\sum_{k=1}^{\frac{p-1}{2}} k \equiv \sum_{k=1}^{\frac{p-1}{2}} k \mod 2$$

and since $-1 \equiv 1 \bmod 2$,
$$\sum_{j=1}^{n} s_j \equiv -\sum_{j=1}^{n} s_j \mod 2$$

and finally $p \equiv 1 \bmod 2$ as well.

so
$$n + \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_j \equiv np + \sum_{i=1}^{m} r_i - \sum_{j=1}^{n} s_j \mod 2$$
$$= \sum_{k=1}^{\frac{p-1}{2}} k$$
$$\equiv \sum_{k=1}^{p-1/2} ka \quad \mod 2$$
$$= p\sum_{k=1}^{p-1/2} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_j$$
$$\equiv \sum_{k=1}^{p-1/2} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_j \mod 2$$

Subtracting $\sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_j$ from both sides,

we get

$$n \equiv \sum_{k=1}^{p-1/2} \left\lfloor \frac{kq}{p} \right\rfloor \mod 2$$

which is what we wanted $\square$

Quadratic Reciprocity. Theorem 9.9
Let p, q be odd primes, $p \neq q$. Then

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

proof: By the Technical lemma

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

So it suffices to show that

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

Key idea: Both sides are the number of integer points in the rectangle

$$\{(x,y) : 0 < x < p/2 ,\ 0 < y < q/2\}$$

Left hand side: if $x, y \in \mathbb{Z}$

since $\left\lfloor \frac{p}{2} \right\rfloor = \frac{p-1}{2}$; then

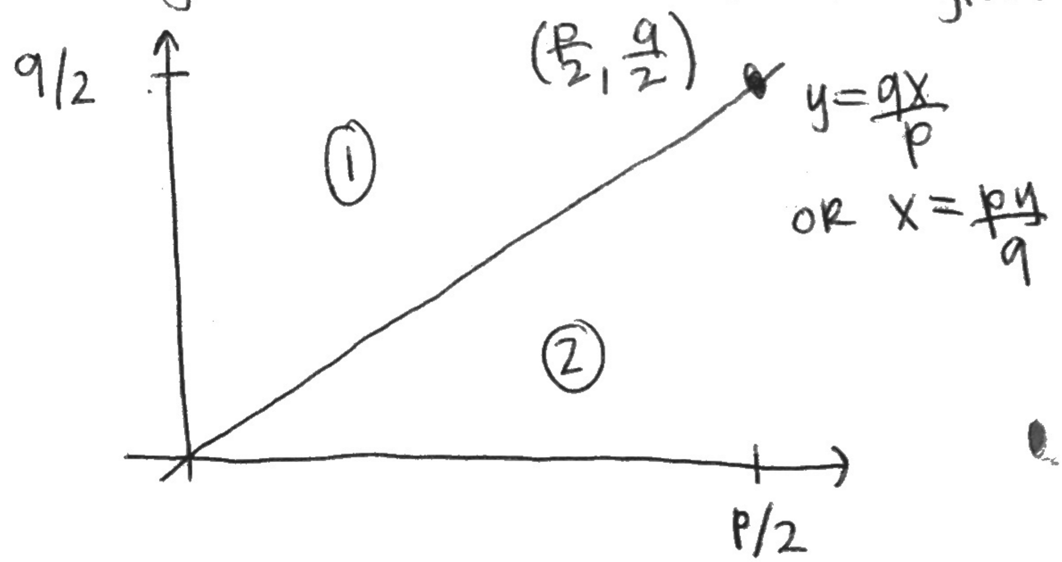
$$0 < x < p/2 \Rightarrow 1 \leq x \leq \frac{p-1}{2}$$

since $\left\lfloor \frac{q}{2} \right\rfloor = \frac{q-1}{2}$, then

$$0 < y < q/2 \Rightarrow 1 \leq y \leq \frac{q-1}{2}$$

A $\frac{p-1}{2}$ by $\frac{q-1}{2}$ grid has $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$

Right hand side: The number of points in the rectangle are divided into two triangles:



Number of integer points in 1:

Fix $0 < y < \frac{q}{2}$ $\left(1 \le y \le \frac{q-1}{2} \text{ since } y \in \mathbb{Z}\right)$

then $0 < x < \frac{py}{q}$ OR

$$1 \le x \le \left\lfloor \frac{py}{q} \right\rfloor \quad \text{since } x \in \mathbb{Z}$$

So number of points in 1 is

$$\sum_{y=1}^{q-1/2} \left\lfloor \frac{py}{q} \right\rfloor = \sum_{k=1}^{q-1/2} \left\lfloor \frac{pk}{q} \right\rfloor$$

Similarly for 2

Fix $1 \le x \le \frac{p-1}{2}$ then

$0 < y < \frac{qx}{p}$ OR $1 \le y \le \left\lfloor \frac{qx}{p} \right\rfloor$

So the number of points in 2 is

$$\sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{qk}{p} \right\rfloor$$

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