Proof of Theorem 63. We need only prove (iii) in view of Lemmas 61 and 62. By Gauss’s Lemma 60,
\( \left( \frac{q}{p} \right) = \left( \frac{-1}{q} \right)^{\mu_q} \), and \( \left( \frac{p}{q} \right) = \left( \frac{-1}{p} \right)^{\mu_p} \). I think it is instructive to take an example \( p = 29, q = 7 \). Then
\[
\begin{align*}
\mathcal{T}_{29} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\} \\
7\mathcal{T}_{29} &= \{7, 14, -8, -1, 6, 13, -9, -2, 5, 12, -10, -3, 4\}
\end{align*}
\]
Note that negative signs occur when \( 7i \) is first greater than \( (2r-1) \frac{29}{7} \), that is when the integer \( i \) is first greater than an odd multiple of \( \frac{29}{14} \) and the number of minus signs is the number of integers \( i \) such that
\[
\frac{(2r-1)29}{2.7} < i < \frac{2r.29}{2.7}.
\]
In general, since the end points of the intervals are never integers, it is clear that in general \( \mu_q \) is the number of integers \( i \) in the intervals,
\[
\frac{(2r-1)p}{2q} < i < \frac{2rp}{2q}.
\]
Similarly, \( \mu_p \) is the number of integers \( i \) in the intervals
\[
\frac{(2r-1)q}{2p} < i < \frac{2rq}{2p}.
\]
To see a connection between the quadratic character of \( q \) modulo \( p \) and the quadratic character of \( p \) modulo \( q \), we need to count the number \( \mu_p \) of integers \( i \) which lie in the intervals
\[
\frac{(2r-1)q}{2p} < i < \frac{2rq}{2p}.
\]
There is absolutely no reason why these two numbers should be the same. For example, if \( p \) is large and \( q \) is small, there may be many integers in the interval \( \left( \frac{(2r-1)p}{2q}, \frac{2rp}{2q} \right) \) and few integers in \( \left( \frac{(2r-1)q}{2p}, \frac{2rq}{2p} \right) \). Hence we cannot expect that \( \mu_p = \mu_q \), for different primes \( p \) and \( q \). Luckily, we don’t have to show this! That the two numbers have the same parity suffices for our needs.

Lemma 64 If \( p \) and \( q \) are primes such that \( p \equiv \pm q \pmod{4a} \), then \( \left( \frac{a}{p} \right) = \left( \frac{a}{q} \right) \). That is, the quadratic character of \( a \) modulo \( p \) is not determined by the prime \( p \) but by the residue of \( p \) modulo \( 4a \).
Proof. Following our example with $q = 7$ and $p = 29$ above, to find $\left( \frac{a}{p} \right)$ for a general prime $p$, using Gauss’s Lemma, we need to count the number of integers $i$ which lie satisfy:

\[ \frac{p}{2} < ai \leq \frac{2p}{2} \]
\[ \frac{3p}{2} < ai \leq \frac{4p}{2} \]
\[ \frac{5p}{2} < ai \leq \frac{6p}{2} \]
\[ \vdots \]

That is, we need to count the number of integers $i$ which satisfy:

\[ \frac{p}{2a} < i \leq \frac{2p}{2a} \]
\[ \frac{3p}{2a} < i \leq \frac{4p}{2a} \]
\[ \frac{5p}{2a} < i \leq \frac{6p}{2a} \]
\[ \vdots \]

That is, to find $\left( \frac{a}{p} \right)$ using Gauss’s Lemma, we need to count the number of integers in the intervals

\[ \left( \frac{p}{2a} : \frac{2p}{2a} \right) \cup \left( \frac{3p}{2a} : \frac{4p}{2a} \right) \cup \left( \frac{5p}{2a} : \frac{6p}{2a} \right) \cup \ldots. \]

Notice that we need $\frac{2kp}{2} \leq \frac{a(p-1)}{2}$ and so there are exactly the integer part of $\frac{a}{2}$ intervals in all. Notice also that since $(a, p) = 1$, the end points of these intervals are never integers.

Similarly, to find $\left( \frac{a}{q} \right)$ using Gauss’s Lemma, we need to count the number of integers in the intervals

\[ \left( \frac{q}{2a} : \frac{2q}{2a} \right) \cup \left( \frac{3q}{2a} : \frac{4q}{2a} \right) \cup \left( \frac{5q}{2a} : \frac{6q}{2a} \right) \cup \ldots. \]

Again there are exactly the integer part of $\frac{a}{2}$ intervals in all and so the number of intervals involved in the calculation of $\mu_p$ and $\mu_q$ does not depend on the primes $p$ and $q$.

There can be no question that these two counts for different $p$ and $q$ can possibly give the same number of integers in each case. We do not try to prove this. We content ourselves with showing that the number of integer points in each of the unions of intervals has the same parity, even or odd. Gauss’s Lemma then shows that

\[ \left( \frac{a}{p} \right) = \left( \frac{a}{q} \right). \]
Case 1. Suppose that $p \equiv q \pmod{4a}$ and so that $p = 4ar + q$, where $r$ is an integer. Then to calculate $\left(\frac{a}{p}\right)$ using Gauss’s Lemma, we need to count the number of integers in the intervals

$$\left(2r + \frac{q}{2a}, 4r + \frac{2q}{2a}\right] \cup \left(6r + \frac{3q}{2a}, 8r + \frac{4q}{2a}\right] \cup \left(10r + \frac{5q}{2a}, 12r + \frac{6q}{2a}\right] \cup \ldots = I_1 \cup I_2 \cup \ldots \cup I_k.$$ 

Here $k$ is the integer part of $\frac{a}{2}$ and so is independent of $q$.

Write the interval $I_1 = \left(2r + \frac{q}{2a}, 4r + \frac{2q}{2a}\right]$ as a union of two subintervals of the following form:

$$I_1 = \left(2r + \frac{q}{2a}, 4r + \frac{2q}{2a}\right] = \left(2r + \frac{q}{2a}, 4r + \frac{q}{2a}\right] \cup \left(4r + \frac{q}{2a}, 4r + \frac{2q}{2a}\right] = J'_1 \cup J_1,$$

where

$$J'_1 = \left(2r + \frac{q}{2a}, 4r + \frac{q}{2a}\right]$$

and

$$J_1 = \left(4r + \frac{q}{2a}, 4r + \frac{2q}{2a}\right].$$

Now $J'_1$ is an interval of length $2r$ with end points which are not integers and so it contains an even number of integer points.

Also $J_1$ contains the same number of integer points as the interval $\left(\frac{q}{2a}, \frac{2q}{2a}\right]$, translating it by the integer distance $-4r$. Again the end points are never integers.

Notice that there is no question that the intervals $I_1 = \left(2r + \frac{q}{2a}, 4r + \frac{2q}{2a}\right]$ and the interval $J_1 = \left(\frac{q}{2a}, \frac{2q}{2a}\right]$ have the same number of integer points! However, the number of integer points in the interval $I_1$ is either even or odd, according as the number of integer points in $J_1$ is even or odd.

Similarly we can write

$$I_2 = \left(6r + \frac{3q}{2a}, 8r + \frac{4q}{2a}\right] = \left(6r + \frac{3q}{2a}, 8r + \frac{3q}{2a}\right] \cup \left(8r + \frac{q}{2a}, 8r + \frac{4q}{2a}\right] = J'_2 \cup J_2,$$

where

$$J'_2 = \left(6r + \frac{3q}{2a}, 8r + \frac{3q}{2a}\right]$$

and
\[ J_2 = \left( 8r + \frac{3q}{2a}, 8r + \frac{4q}{2a} \right). \]

Now \( J'_2 \) is an interval of length 2\( r \) with end points which are not integers and so contains an even number of integer points.

Also \( J_2 \) contains the same number of integer points as the interval \( \left( \frac{3q}{2a}, \frac{4q}{2a} \right) \), translating it by the distance \(-8r\). Again the end points are never integers.

Again there is no question that the intervals \( I_2 = \left( 6r + \frac{3q}{2a}, 8r + \frac{4q}{2a} \right) \) and the interval \( J_2 = \left( \frac{3q}{2a}, \frac{4q}{2a} \right) \) have the same number of integer points! But the number of integer points in the interval \( I_2 \) is either even or odd, according as the number of integer points in \( J_2 \) is even or odd.

And so on for the remaining intervals.

It is clear that the number of integer points in the intervals \( I_1 \cup I_2 \cup \ldots \) has the same parity, even or odd, as the number of integer points in the intervals \( J_1 \cup J_2 \cup \ldots \).

Hence \( \left( \frac{a}{p} \right) = \left( \frac{a}{q} \right) \), if \( p = 4ar + q \).

Case 2. Suppose that \( p \equiv -q \pmod{4a} \) and so that \( p = 4ar - q \), where \( r \) is an integer.

Remark: I will not go through this proof in class. It is very similar to the case above, with just a slight twist. I include it here for completeness.

This is just slightly different from Case 1 and can be followed rather easily when Case 1 is understood. It can almost be done by cutting and pasting!

To calculate \( \left( \frac{a}{p} \right) \) using Gauss’s Lemma, we need to count the number of integers in the intervals

\[ I_1 \cup I_2 \cup \ldots, \] where with an obvious notation. \( I_k = \left( (2k + 1)\frac{p}{2a}, 2k \frac{p}{2a} \right). \)

\[ \left( \frac{p}{2a}, \frac{2p}{2a} \right) \cup \left( \frac{3p}{2a}, \frac{4p}{2a} \right) \cup \left( \frac{5p}{2a}, \frac{6p}{2a} \right) \cup \ldots \]

\[ \left( 2r - \frac{q}{2a}, 4r - \frac{2q}{2a} \right) \cup \left( 6r - \frac{3q}{2a}, 8r - \frac{4q}{2a} \right) \cup \left( 10r - \frac{5q}{2a}, 12r - \frac{6q}{2a} \right) \cup \ldots = I_1 \cup I_2 \cup \ldots \cup I_k. \]

Here \( k \) is the integer part of \( \frac{a}{2} \) and so is independent of \( q \).

Consider

\[ \left( 2r - \frac{q}{2a}, 4r - \frac{q}{2a} \right) = \left( 2r - \frac{q}{2a}, 4r - \frac{2q}{2a} \right) \cup \left( 4r - \frac{2q}{2a}, 4r - \frac{q}{2a} \right), \] that is,

\[ J'_1 = I_1 \cup J_1, \]
where

\[ J'_1 = \left( 2r - \frac{q}{2a}, 4r - \frac{q}{2a} \right) \] and

\[ J_1 = \left( 4r - \frac{2q}{2a}, 4r - \frac{q}{2a} \right). \]

Now \( J'_1 \) is an interval of length \( 2r \) with end points which are not integers and so contains an even number of integer points.

Also \( J_1 \) contains the same number of integer points as the interval \( \left( -\frac{2q}{2a}, -\frac{q}{2a} \right) \), translating it by the distance \( 4r \). Again the end points are never integers. Hence the number of integer points in \( J_1 \) is the same as the number of integer points in the open interval \( \left( -\frac{2q}{2a}, -\frac{q}{2a} \right) \) and this is the same as the number of integer points in the open interval \( \left( \frac{q}{2a}, \frac{2q}{2a} \right) \), multiplying the interval by \(-1\). This is again the same as the number of integer points in the interval \( \left( \frac{q}{2a}, \frac{2q}{2a} \right) \).

Thus the number of integers in the interval \( \left( -\frac{2q}{2a}, -\frac{q}{2a} \right) \), is the same as the number of integers in the interval \( \left( \frac{p}{2a}, \frac{2p}{2a} \right) \) is the same modulo 2 as the number of integer points in the interval \( \left( \frac{q}{2a}, \frac{2q}{2a} \right) \).

Similarly,

\[ \left( 6r - \frac{3q}{2a}, 8r - \frac{3q}{2a} \right) = \left( 6r - \frac{3q}{2a}, 8r - \frac{3q}{2a} \right) \cup \left( 8r - \frac{3q}{2a}, 8r - \frac{4q}{2a} \right), \] that is,

\[ J'_2 = I_2 \cup J_2, \]

where

\[ J'_2 = \left( 6r - \frac{3q}{2a}, 8r - \frac{3q}{2a} \right) \] and

\[ J_2 = \left( 8r - \frac{3q}{2a}, 8r - \frac{4q}{2a} \right). \]

Now \( J'_2 \) is an interval of length \( 2r \) with end points which are not integers and so contains an even number of integer points.

Hence the number of integer points in the interval \( I_2 \) is either even or odd, according as the number of integer points in \( J_2 \) is even or odd, since the number of integer points in \( J'_2 = I_2 \cup J_2 \) is even.

And so on for the remaining intervals.

It is clear now that the number of integer points in the intervals

\[ I_1 \cup I_2 \cup \ldots, \]
which depends only on $a$ and $p$ has the same parity, even or odd, as the number of integer points in the intervals $J_1 \cup J_2 \cup \ldots$, which depends only on $a$ and $q$.

Hence $\left( \frac{a}{p} \right) = \left( \frac{a}{q} \right)$, if $p \equiv \pm q \pmod{4a}$, in both cases.

Given the subtlety of the proof of Lemma 64, it is interesting that the Law of Quadratic Reciprocity 63(iii) follows so quickly now.

**Proof of Theorem 63.**

Suppose now that $p$ and $q$ are odd primes. We distinguish four cases.

**Case 1.** $p \equiv q \equiv 1 \pmod{4}$.

Then $p - q = 4r$, for some integer $r$ and so $q = p - 4r$ and $p \equiv q \pmod{4r}$.

Then

\[
\left( \frac{q}{p} \right) = \left( \frac{p - 4r}{p} \right) = \left( \frac{-4r}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{4}{p} \right) \left( \frac{r}{p} \right)
\]

By Theorem 63(i) (or by Gauss’s §108, $\left( \frac{-1}{p} \right) = 1$, since $p \equiv 1 \pmod{4}$). Also, $\left( \frac{4}{p} \right) = 1$ since 4 is a square modulo $p$.

Hence $\left( \frac{q}{p} \right) = \left( \frac{r}{p} \right)$.

Since $p = q + 4r$,

\[
\left( \frac{p}{q} \right) = \left( \frac{q + 4r}{q} \right) = \left( \frac{4r}{q} \right) = \left( \frac{4}{q} \right) \left( \frac{r}{q} \right)
\]

Since 4 is a square modulo $q$, $\left( \frac{4}{q} \right) = 1$. Hence $\left( \frac{p}{q} \right) = \left( \frac{r}{q} \right)$.

By Lemma 64, $\left( \frac{y}{p} \right) = \left( \frac{r}{q} \right)$ because $p \equiv q \pmod{4r}$, and so $\left( \frac{p}{q} \right) = \left( \frac{q}{p} \right)$.

**Case 2.** $p \equiv 1 \pmod{4}$, $q \equiv 3 \pmod{4}$ Then $p + q \equiv 0 \pmod{4}$ and so $p + q = 4r$, for some integer $r$. Then, since $q = 4r - p$,
\[
\left( \frac{q}{p} \right) = \left( \frac{4r - p}{p} \right) \\
= \left( \frac{4r}{p} \right) \\
= \left( \frac{4}{p} \right) \left( \frac{r}{p} \right)
\]

\[
\left( \frac{4}{p} \right) = 1 \text{ since } 4 \text{ is a square modulo } p \text{ and so } \left( \frac{q}{p} \right) = \left( \frac{r}{p} \right).
\]

Since \( p = 4r - q \),

\[
\left( \frac{p}{q} \right) = \left( \frac{4r - q}{q} \right) \\
= \left( \frac{4r}{q} \right) \\
= \left( \frac{4}{q} \right) \left( \frac{r}{q} \right)
\]

Since 4 is a square modulo \( q \), \( \left( \frac{4}{q} \right) = 1 \). Hence \( \left( \frac{p}{q} \right) = \left( \frac{r}{q} \right) \).

By Lemma 64, \( \left( \frac{y}{p} \right) = \left( \frac{r}{q} \right) \) because \( p \equiv -q \pmod{4r} \), and so \( \left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) \).

**Case 3.** \( q \equiv 1 \pmod{4} \), \( p \equiv 3 \pmod{4} \)

This is clearly similar to Case 2 and presents no difficulty.

**Case 4.** \( p \equiv q \equiv 3 \pmod{4} \).

Then \( p - q \equiv 0 \pmod{4} \) and so \( p - q = 4r \) for some integer \( r \). Hence \( p = q + 4r \) and so

\[
\left( \frac{p}{q} \right) = \left( \frac{q + 4r}{q} \right) \\
= \left( \frac{4r}{q} \right) \\
= \left( \frac{4}{q} \right) \left( \frac{r}{q} \right)
\]

\[
\left( \frac{4}{p} \right) = 1 \text{ since } 4 \text{ is a square modulo } p.
\]

Hence \( \left( \frac{p}{q} \right) = \left( \frac{r}{q} \right) \).
Since \( q = p - 4r \),

\[
\left( \frac{q}{p} \right) = \left( \frac{p - 4r}{p} \right) = \left( \frac{-4r}{p} \right) = \left( \frac{-1}{q} \right) \left( \frac{4}{q} \right) \left( \frac{r}{q} \right)
\]

By Theorem 63(i) (or Gauss’s §108), \( \left( \frac{-1}{q} \right) = -1 \), since \( q \equiv 3 \pmod{4} \).

Since 4 is a square modulo \( q \), \( \left( \frac{4}{q} \right) = 1 \). Hence \( \left( \frac{p}{q} \right) = - \left( \frac{r}{q} \right) \).

By Lemma 64, \( \left( \frac{y}{p} \right) = \left( \frac{r}{q} \right) \) because \( p \equiv q \pmod{4r} \), and so \( \left( \frac{p}{q} \right) = - \left( \frac{q}{p} \right) \), if \( p \equiv q \equiv 3 \pmod{4} \).

This completes the proof of the Law of Quadratic Reciprocity.

Gauss gave 8 different proofs of the Law of Quadratic Reciprocity during his life. It has since been proved in more than 150 different ways. It has also formed a basis for a great deal of the development of mathematics in the past 167 years since his death.