9. Quadratic equations mod p, p an odd prime

(9.1)

Consider a general quadratic equation mod p: $ax^2+bx+c \equiv 0 \pmod p$ ... (1), $(p, a)=1$. Then, $(p, 4a)=1$ and (1) has a solution $x \pmod p$ if, and only if

$$4a(ax^2+bx+c) \equiv 0 \pmod p$$

has a solution $\pmod p$; i.e.,

$$(2ax+b)^2 = b^2-4ac \pmod p \quad \dots (2)$$

has a solution. Put $X = 2ax+b$ and $d = b^2-4ac$. Then, (2) can be written as

$$X^2 \equiv d \pmod p \quad \dots (3)$$

If $x = x_0$ satisfies (1), then $x_1 = 2ax_0+b$ satisfies (3). On the other hand, if x_2 is a solution to (3), then the solution to

$2ax = x_4 - b$ is a solution to (1).

So, solving (1) and (3) are equivalent. We study when equations of type (3) can be solved.

Example. Solve $5x^2 - 6x + 2 \equiv 0 \pmod{13}$ — (1)

Solution: Put $Y = 10x - 6$, $d = 36 - 40 = 9 \pmod{13}$

(1) can be solved if $Y^2 \equiv 9 \pmod{13}$ ... (3) can be solved.

$Y = 3$ and $Y = 10$ are solutions to (3) $\pmod{13}$.

For $10x - 6 \equiv 3 \pmod{13}$, $x \equiv 10 \pmod{13}$ is the soln.

For $10x - 6 \equiv 10 \pmod{13}$, i.e., $10x \equiv 3 \pmod{13}$,

$x \equiv 12 \pmod{13}$ is the solution. □

Exc: Solve (i) $x^2 + 7x + 10 \equiv 0 \pmod{11}$.

(ii) $5x^2 + 6x + 1 \equiv 0 \pmod{23}$.

MAIN PROBLEM: When does $X^2 \equiv a \pmod{p}$ has a soln? p - an odd prime, $(p, a) = 1$.

Quadratic reciprocity Law

Let p be an odd prime and $a \in \mathbb{Z}$ such that $\gcd(a,p)=1$. This law (due to Gauss) enables us to decide if the Congruence $X^2 \equiv a \pmod p$ has a solution. — (1)

DEF: We say that a is a quadratic residue mod p (written aRp) if (1) has a solution (mod p); i.e., there exists $e \in \mathbb{Z}$ such that $e^2 \equiv a \pmod p$. We say that a is a quadratic non residue (mod p) (and write aNp) if it is not a quadratic residue mod p.

$X^2 = a \pmod p$ $X^2 \equiv b \pmod p$

Note. If $a \equiv b \pmod p$, $aRp \iff bRp$. So, we only consider the quadratic character of elements of $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$.

1. Euler's criteria Let p be an odd prime and $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$. Then, aRp iff $a^{(p-1)/2} \equiv 1 \pmod p$.

Proof. (i) Let aRp and x_1 be a solution mod p to $x^2 \equiv a \pmod p$. Since $(p, a) = 1$, $x_1^2 \equiv a \pmod p$ $(p, x_1) = 1$.

By Fermat's theorem,

$$a^{(p-1)/2} \equiv (x_1^2)^{(p-1)/2} = x_1^{p-1} \equiv 1 \pmod p.$$

(ii) Now assume $a^{(p-1)/2} \equiv 1 \pmod p$.

Let r be a primitive root mod p; i.e., $\mathbb{Z}_p^* = \langle r \rangle$.

Then, $a = r^t$ for some integer t with $1 \le t \le p-1$ and

9.3

$$a^{(p-1)/2} \equiv (r^t)^{(p-1)/2} = r^{t(p-1)/2} \equiv 1 \pmod{p}$$

Since $(p-1)$ is the smallest positive integer n such that $r^n \equiv 1 \pmod{p}$, $(p-1)$ divides $(p-1)t/2$. So, t is even, say $t = 2k$, $k \in \mathbb{Z}$ and $r^k \pmod{p}$ is a solution to $x^2 \equiv a \pmod{p}$. So, aRp. □

Remark. Since p is odd and $(p, a) = 1$, using Fermat's theorem,

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Since $\mathbb{Z}_p$ is an integral domain, either

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \text{or} \quad a^{(p-1)/2} \equiv -1 \pmod{p}$$

for each $a \in \mathbb{Z}$ with $p \nmid a$.

However, both can not happen; otherwise, if 9.6 both hold for some a, then $1 \equiv -1 \pmod{p}$ and $p \mid 2$, a contradiction. □

Ex. $2 \mathbb{N} 13$ because $2^{(13-1)/2} = 2^6 \equiv 64 \equiv 12 \equiv -1 \pmod{13}$ □

Legendre Symbol

Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$.

Write $(a/p) = 1$ or -1 according as $a \mathbb{R} p$ or $a \mathbb{N} p$.

(a/p) is called the Legendre Symbol of a relative to p. It is also written as $\left(\frac{a}{p}\right)$

Ex: $\left(\frac{a}{13}\right) = 1$ for $a \in \{1, 3, 4, 9, 10, 12\}$

$\left(\frac{a}{13}\right) = -1$ for $a \in \{2, 5, 6, 7, 8, 11\}$.

Convention: $\left(\frac{a}{p}\right)$ is taken as zero if $p \mid a$. Then, $x^2 \equiv a \pmod{p}$ has $1 + \left(\frac{a}{p}\right)$ solutions $\pmod{p}$ for all $a \in \mathbb{Z}$.

Theorem: Let p be an odd prime and $a, b \in \mathbb{Z}$ be such that $(p, a) = 1 = (p, b)$. Then:

(i) $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) $\left(\frac{a^2}{p}\right) = 1$; (iii) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$

(iv) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

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

(vi) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

Proof. Exercise. □

So, $3 \mathcal{N} 17$ and $x^2 \equiv -46 \pmod{17}$ has NO solution

Cor: $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4. \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$

Ex: $\left(\frac{-46}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{46}{17}\right) = \left(\frac{46}{17}\right) \overset{(ii)}{=} \left(\frac{12}{17}\right) = \left(\frac{3 \times 2^2}{17}\right) \overset{(vi)}{=} \left(\frac{3}{17}\right)$.

Now, $3^8 \equiv (81)^2 \equiv (-4)^2 \equiv -1 \pmod{17}$.

Before we give a proof, some examples and an application:

Ex1: Let $p=13$ and $a=5$. Then, $(p-1)/2=6$ and $S=\{5, \underline{10}, 2, \underline{7}, \underline{12}, 4\}$. So, $n=3$ and $\left(\frac{5}{13}\right)=(-1)^3=-1$. So, $x^2\equiv 5 \pmod{13}$ has no solutions.

Ex2: $\left(\frac{2}{p}\right)=\begin{cases} 1 & \text{if } p\equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } p\equiv 3 \text{ or } 5 \pmod 8 \end{cases}$

Proof: $S=\{2, 2\times 2, 2\times 3, \ldots, 2\times\frac{p-1}{2}\}$

observe that each element of S is less than p.

So, $n=|\{s\in S: s>p/2\}|=\frac{p-1}{2}-\left[\frac{p}{4}\right]$

because, for $1\le t\le \frac{p-1}{2}$, $2t<\frac{p}{2}$ if $t<\left[\frac{p}{4}\right]$.

Now,

$p=8r+1 \Rightarrow n=4r-2r=2r$

$p=8r+3 \Rightarrow n=(4r+1)-2r=2r+1$

$p=8r+5 \Rightarrow n=(4r+2)-(2r+1)=2r+1$

$p=8r+7 \Rightarrow n=(4r+3)-(2r+1)=2r+2$. □

An application: There are an infinite number of primes of the form $4k+1$.

Proof: Deny. Suppose that $p_1, \dots, p_n$ are the only primes of the form $4k+1$. Let $N = (2p_1 \cdots p_n)^2 + 1$. Since N is odd, there exists an odd prime p dividing N. In other words,

$$(2p_1 \cdots p_n)^2 \equiv -1 \pmod{p}.$$

So, $\left(\frac{-1}{p}\right) = 1$. So, the Corollary implies $p = 4t+1$ for some $t \in \mathbb{Z}$ and so, $p = p_i$ for some i. This then implies $p \mid N - (2p_1 \cdots p_n)^2 = 1$, an impossibility. So, our hypothesis that there are only finite numbers of the form $4k+1$ is not true. □

Note: In 1837, Dirichlet proved that Arithmetic progression $\{kn+h : n = 1, 2, \dots\}$ has an infinite number of primes iff $\gcd(k, h) = 1$.

GAUSS Lemma. Although Euler's criteria suggests a method to decide the quadratic nature of an integer a modulo a prime p, the computing $a^{\frac{p-1}{2}} \bmod p$ could be very unwieldy if p is large. The following result due to Gauss (of which he was justifiably very proud) is computationally more feasible and most proofs of quadratic reciprocity law uses it.

Theorem (Gauss Lemma): Let p be an odd prime and $a \in \mathbb{Z}$ such that $(a, p) = 1$. Let n denote the number of elements in the set

$$S = \{a, 2a, \ldots, \tfrac{p-1}{2}a\}$$

which when divided by p leaves the remainder greater than $p/2$. Then, $\left(\frac{a}{p}\right) = (-1)^n$.

Proof of Gauss Lemma: Since $(p, a)=1$, each element of S is nonzero congruent (modulo p) and no two elements of S congruent (modulo p).

On dividing each element of S by p, let $\{r_1, \cdots, r_t\}$ be the remainders such that $1 \leq r_i < \frac{p}{2}$ and $\{s_1, \cdots, s_m\}$ ——— " ——— $\frac{p}{2} < s_j \leq p-1$.

Then, $t+m = (p-1)/2$ and, for all i, j, $r_i \neq p - s_j$.

(In fact, if $r_i = p - s_j \Rightarrow p = r_i + s_j$. Let u, v be integers, $1 \leq u, v \leq (p-1)/2$ such that $s_j \equiv ua \pmod{p}$ and $r_i \equiv va \pmod{p}$, then $(u+v)a = r_i + s_j = p \equiv 0 \pmod{p}$ which is impossible because $(a, p)=1$ and $1 \leq u+v \leq p-1$.)

So, $\{r_1, \cdots, r_t\}$ and $\{p-s_1, \cdots, p-s_m\}$ are disjoint subsets of $\{1, \cdots, (p-1)/2\}$ and $t+m = (p-1)/2$. So,

$$\{1, \cdots, (p-1)/2\} = \{r_1, \cdots, r_t; p-s_1, \cdots, p-s_m\}.$$

Now, $\left(\frac{p-1}{2}\right)! = (r_1 \cdots r_t)(p-s_1)\cdots(p-s_m)$

$\equiv (r_1 \cdots r_t)(s_1 \cdots s_m)(-1)^m \pmod p$

$\equiv (-1)^m a \times 2a \times \cdots \times \left(\frac{p-1}{2}\right)a \pmod p$

$\equiv (-1)^m a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p.$

Since $\gcd\left(p, \left(\frac{p-1}{2}\right)!\right) = 1$, $a^{(p-1)/2} \equiv (-1)^m \pmod p.$

Now, by Euler's criteria, $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} = (-1)^m \pmod p.$ □

An application: There are an infinite number of primes of the form $8k-1$.

Proof. Deny. Suppose that $p_1, p_2, \cdots, p_l$ are the only primes of the form $8k-1$. Let $N = (4p_1 \cdots p_l)^2 - 2$.

→ Then, there is at least one odd prime p which divides N. So, $x^2 \equiv 2 \pmod{p}$ has a solution, $(4p_1 \cdots p_l) \bmod p$; i.e., $\left(\frac{2}{p}\right) = 1$. Consequently, by Ex.2, $p \equiv 1$ or $7 \pmod 8$.

→ If all (odd) prime divisors of N are of the form $8t+1$, then N would be of the form $2(8q+1) = 16q+2 \equiv 2 \pmod{16}$. But, N is of the form $16b-2$. But this is impossible, otherwise, $16a+2 \equiv 16b-2 \pmod{16}$ and $16 \mid 4$ →←

→ So, N has at least one prime divisor p of the form $8t-1$. But, then $p = p_i$ for some i, and so $p \mid 2$, a contradiction. □

Def. For $r \in \mathbb{R}$, the integral part $\lfloor r \rfloor$ of r is the largest integer less than or equal to r. The fractional part $\{r\} = r - \lfloor r \rfloor$.

Ex: $\lfloor 3/2 \rfloor = 1 = \lfloor 1 \rfloor$, $\lfloor -1/2 \rfloor = -1 = \lfloor -1 \rfloor$

$\{3/2\} = \frac{1}{2}$, $\{1\} = \{-1\} = 0$, $\{-1/2\} = 1/2$.

We state and prove Gauss lemma in a slightly more general form: We give another expression for m.

Thm. Let p be an odd prime; $a \in \mathbb{Z}$ with $(p, a) = 1$ and $m \in \mathbb{N}$ defined as in the earlier statement. Then,

$$m = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor + (a-1)\frac{p^2-1}{8} \pmod 2 \quad -(*)$$

In particular, if a is odd,

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

Proof. We continue with the notation of the Gauss lemma:

- $S = \{a, 2a, \cdots, a\frac{p-1}{2}\}$
- $\{r_1, \cdots, r_t\}$ and $\{s_1, \cdots, s_m\}$ the set of remainders $< p/2$ and the set of remainders $> p/2$, respectively, on dividing elements of S by p. We saw:

$$\{r_1, \cdots, r_t\} \cup \{p - s_1, \cdots, p - s_m\} = \{1, \cdots, \frac{p-1}{2}\}$$

So,
$$\sum_{k=1}^{(p-1)/2} k = \sum_{i=1}^{t} r_i + pm - \sum_{j=1}^{m} s_j \quad \cdots \quad (1)$$

For $k = 1, \cdots, (p-1)/2$, $ka = p\left\lfloor \frac{ka}{p} \right\rfloor + l_k$, $0 \le l_k \le p-1$.

So,
$$a \sum_{k=1}^{(p-1)/2} k = p\left(\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor\right) + \sum_{i=1}^{t} r_i + \sum_{j=1}^{m} s_j \quad \cdots (2)$$

Substracting (1) from (2), we get

$$(a-1)\sum_{k=1}^{(p-1)/2} k = p\left(\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor\right) - pm + 2\sum_{j=1}^{m} s_j .$$

Considering this modulo 2 and observing $p \equiv 1 \pmod 2$ and $1+2+\cdots+\frac{p-1}{2} = \frac{p^2-1}{8}$, (*) follows.

The second part is clear. □

We now come to the quadratic reciprocity law. This has fascinated so much so that there are at least 150 proofs known, Gauss himself contributing 8 proofs.

Theorem (Gauss) Let p, q be distinct odd primes. Then,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Proof: By Gauss lemma and previous theorem

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{m+n}$ where $m = \sum_{t=1}^{(q-1)/2} \left\lfloor \frac{qt}{p} \right\rfloor$ and $n = \sum_{s=1}^{(p-1)/2} \left\lfloor \frac{ps}{q} \right\rfloor$.

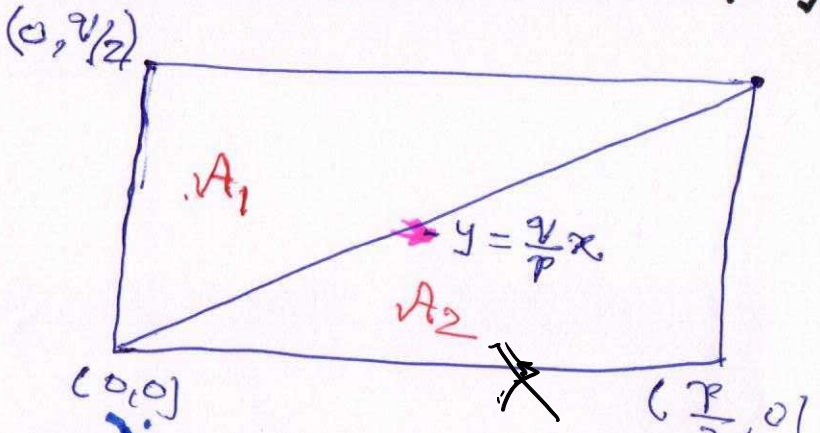
To complete the proof, we show: $m+n = \frac{p-1}{2}\cdot\frac{q-1}{2}$.

Let

$A := \{(x,y) \in \mathbb{Z}^2 : 1 \le x \le \frac{p-1}{2} \text{ and } 1 \le y \le \frac{q-1}{2}\}$

$A_1 := \{(x,y) \in A : qx > py\}$; $A_2 := \{(x,y) \in A : qx < py\}$.

- A has no point on the diagonal; i.e., there is no point $(a,b) \in A$ such that $pb = qa$.
  (If so, then $p \mid a$ and $1 \le a < \frac{p-1}{2}$ ↯)



- A_1 and A_2 are elements of A on either side of the diagonal and so $A = A_1 \sqcup A_2$.

- $A_1 = \{(x,y): 1 \le x \le \frac{p-1}{2},\ 1 \le y \le \lfloor \frac{qx}{p} \rfloor\}$

  $A_2 = \{(x,y): 1 \le y \le \frac{q-1}{2},\ 1 \le x \le \lfloor \frac{py}{q} \rfloor\}$

  $\frac{p-1}{2} \cdot \frac{q-1}{2} = |A| = |A_1| + |A_2| = \sum_{t=1}^{(p-1)/2} \lfloor \frac{qt}{p} \rfloor + \sum_{s=1}^{(q-1)/2} \lfloor \frac{ps}{q} \rfloor$. Now □

<u>Remarks.</u> The above theorem says.

$pRq \iff qRp$ if p or $q \equiv 1 \pmod 4$

$pRq \iff qNp$ if q and $p \equiv -1 \pmod 4$

$pNq \iff qNp$ if p or $q \equiv 1 \pmod 4$

- In other words, if either p or q is of the form $4t+1$, then either both $x^2 \equiv p \pmod q$ and $x^2 \equiv q \pmod p$ have solutions or both do not have solutions
- If both p and q are of the form $4t+3$, then one, and only one, of $x^2 \equiv p \pmod q$ and $x^2 \equiv q \pmod p$ has a solution.

Ex: $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right)$

$= -\left(\frac{29}{7}\right) \equiv -\left(\frac{1}{7}\right) = -1.$

Exc. Show that $\left(\frac{-42}{61}\right) = 1.$

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

(ii) We can also use the quadratic reciprocity law to determine which primes q have the property that a given prime p is a quadratic residue mod q.

Ex. Let $p = 3$. To find the primes q such that $\left(\frac{3}{q}\right) = 1$.

Note that $\left(\frac{3}{q}\right) = \left(\frac{q}{3}\right)(-1)^{(q-1)/2}$ (by $(*)$)

$\left(\frac{q}{3}\right) = \left(\frac{1}{3}\right) = 1$ if $q \equiv 1 \pmod 3$

$\left(\frac{q}{3}\right) = \left(\frac{2}{3}\right) = -1$ if $q \equiv 2 \pmod 3$

and $(-1)^{(q-1)/2} = 1$ or -1 according as $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$

So, $\left(\frac{3}{q}\right)=1 \iff \begin{cases} q \equiv 1 \pmod 3 \text{ and } q \equiv 1 \pmod 4 \\ \text{or} \\ q \equiv 2 \pmod 3 \text{ and } q \equiv 3 \pmod 4 \end{cases}$

$\iff q \equiv 1 \text{ or } 11 \pmod{12}$.

(Chinese remainder theorem) □

More generally,

Theorem. Let p be an odd prime. For any odd prime $q > p$, define a positive integer r as follows:

- If $p = 4m+1$, take r as the integer such that $q = pt + r$, $0 < r < p$, $t \in \mathbb{N}$.
- If $p = 4m+3$, take r to be the unique (positive) integer such that $q = 4pt \pm r$, $0 < r < 4p$ and $r \equiv 1 \pmod 4$

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

QRL $q \equiv r \pmod p$

Proof (i) If $p \equiv 1 \pmod 4$, $\left(\frac{p}{q}\right) \overset{!}{=} \left(\frac{q}{p}\right) \overset{!}{=} \left(\frac{r}{p}\right)$.

(ii) Let $p \equiv 3 \pmod 4$. We first show that r as specified in the theorem exists.

Let $l, r_0 \in \mathbb{Z}$ be such that $q = (4p)l + r_0$, $0 \le r_0 < 4p$.

If $r_0 \equiv 1 \pmod 4$, take $r = r_0$.

If $r_0 \equiv 3 \pmod 4$, then take $r = 4p - r_0$.

Then, $r \equiv 1 \pmod 4$ in each case.

and uniqueness is verified easily.

If $q = 4pk + r$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{r}{p}\right)$.

If $q = 4pk - r$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) = -\left(\frac{-r}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{r}{p}\right)$

$= \left(\frac{r}{p}\right)$. □

Ex. $\left(\frac{38}{43}\right) = \left(\frac{2}{43}\right)\left(\frac{19}{43}\right) = -\left(\frac{19}{43}\right) = \left(\frac{5}{19}\right)\left(\frac{43}{19}\right)$

$= \left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = 1$. So, $38 R 43$.

Alternatively,

$\left(\frac{38}{43}\right) = \left(\frac{2}{43}\right)\left(\frac{19}{43}\right) = -\left(\frac{-24}{43}\right)$ since $19 \equiv -24 \pmod{43}$

$= -\left(\frac{-1}{43}\right)\left(\frac{2^2}{43}\right)\left(\frac{6}{43}\right) = \left(\frac{6}{43}\right) = \left(\frac{49}{43}\right) = 1$.

Exc. Calculate $\left(\frac{36}{109}\right)$, $\left(\frac{7}{103}\right)$. ═

An example: Let $p = 11$. To find all primes q such that $\left(\frac{11}{q}\right) = 1$.

A complete set of quadratic residues r mod 11 such that $0 < r < 44$ and $r \equiv 1 \pmod 4$ are

$$1, 5, 9, 25, 37$$

So, the set of all odd primes q for which 11 is a quadratic residue are all primes of the form $44k \pm r$ with $r \in \{1, 5, 9, 25, 37\}$.