THEORY OF NUMBERS
QUADRATIC RESIDUES

The problem can be reduced to a study of the congruence

$$x^2 \equiv a \bmod p$$

Suppose $a \not\equiv 0 \bmod p$.
If $x^2 \equiv a$ is soluble a is called a quadratic residue mod p.
If $x^2 \equiv a$ is not soluble a is a quadratic non-residue mod p.

The Legendre Symbol $\left(\frac{n}{p}\right) = \begin{cases} +1 & \text{if } n \text{ is quadratic residue mod } p. \\ -1 & \text{if } n \text{ is quadratic non-residue mod } p \\ 0 & \text{if } n \equiv 0 \bmod p \end{cases}$

Theorem $\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = 0$

i.e. $\exists$ the same number of quadratic residues and quadratic non-residues.

Proof $\pm 1, \pm 2, \ldots \pm \frac{1}{2}(p-1)$ form an R.S.R. so $1^2\ 2^2 \ldots \left(\frac{p-1}{2}\right)^2$ contain all the quadratic residues.

$x^2 \equiv y^2 \bmod p \Rightarrow x \equiv \pm y \bmod p$

and this does not occur with the above R.S.R. so these are all the quadratic residues mod p and there are $\frac{p-1}{2}$ of them.

Theorem $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \bmod p$.

Proof $n \equiv 0$ is trivial. If n is a quadratic residue $\exists\ x$ such that $n \equiv x^2$ then $(x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1$ by Fermats theorem. $\exists \frac{p-1}{2}$ quadratic residues and $n^{\frac{p-1}{2}} \equiv 1$ has at most $\frac{p-1}{2}$ solutions therefore the quadratic residues are all the solutions of $n^{\frac{p-1}{2}} = 1$.

Suppose $(n,\ p) = 1$ then $n^{p-1} \equiv 1$ therefore

$\left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right) \equiv 0$ therefore

$n^{\frac{p-1}{2}} \equiv \pm 1$

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

Theorem For every pair of integers $m,\ n$ we have

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$

Proof If $E = \left(\frac{mn}{p}\right) - \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$ then $E \equiv (mn)^{\frac{p-1}{2}} - m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv 0$.

But $|E| \leq 2$ and $p \geq 3$ therefore $E = 0$.

Gauss's Lemma Suppose $n \not\equiv 0 \bmod p$. Let μ be the number of those numbers $1,\ n,\ 2n \ldots \frac{p-1}{2}n$ whose remainder mod p is $> \frac{1}{2}p$. Then $\left(\frac{n}{p}\right) = (-1)^\mu$

Proof Let the remainders $> \frac{1}{2}p$ be $\alpha_1 \ldots \alpha_\mu$. Let those $< \frac{1}{2}p$ be $\beta_1 \ldots \beta_\nu$. Then $\mu + \nu = \frac{p-1}{2}$.

Consider the $\frac{p-1}{2}$ numbers $p - \alpha_1,\ p - \alpha_2 \ldots p - \alpha_\mu,\ \beta_1,\ \beta_2, \ldots \beta_n u$

$1 \leq \beta \leq \frac{p-1}{2}$ and $1 \leq p - \alpha \leq \frac{p-1}{2}$

The β_i are distinct for $k'n \equiv k''n \bmod p \Rightarrow k' \equiv k'' \bmod p,\ (n,\ p) = 1$

Similarly the $p - \alpha_j$ are distinct.

Now $p - \alpha_j \equiv \beta_i \bmod p \Rightarrow \alpha_j + \beta_i \equiv p \equiv 0 \bmod p$. Let $\alpha_j = un\ \beta_i = vn$

Then $(u+v)n \equiv 0 \bmod p$ therefore $u + v \equiv 0 \bmod p$.

But $1 \leq u + v \leq p - 1$ and so we have a contradiction.

Hence $p - \alpha_1,\ p - \alpha_2 \ldots p - \alpha_\mu,\ \beta_1,\ \beta_2 \ldots \beta_\nu$ is a rearrangement of $1, 2, \ldots \frac{p-1}{2}$. Therefore

$$\begin{aligned}
(p - \alpha_1)(p - \alpha_2) \ldots (p - \alpha_\mu)\beta_1 \ldots \beta_\nu &\equiv 1, 2 \ldots \frac{p-1}{2}\ (p) \\
\text{therefore } (-1)^\mu \prod_{j=1}^{\frac{p-1}{2}} jn &\equiv \prod_{j=1}^{\frac{p-1}{2}} j \bmod p \\
\text{therefore } (-1)^\mu n^{\frac{n-1}{2}} &\equiv 1 \bmod p \\
\text{therefore } \left(\frac{n}{p}\right) &\equiv (-1)^\mu \bmod p \\
\text{therefore } \left(\frac{n}{p}\right) &= (-1)^\mu\ p \geq 3
\end{aligned}$$

The Law of Quadratic Reciprocity Suppose $p,\ q$ are distinct odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{p}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

i.e. $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless $p \equiv p \equiv -1 \bmod 4$ when $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Proof 1 Let $p' = \frac{p-1}{2},\ q' = \frac{q-1}{2}$. Write $s = \sum_{m=1}^{p'} \left[\frac{mq}{p}\right]$

For each $m = 1, 2, \dots p'$

$$mq = p\left[\frac{mq}{p}\right] + \left\{\begin{array}{lll} \alpha & \text{if} & > \frac{1}{2}p \\ \beta & \text{if} & < \frac{1}{2}p \end{array}\right.$$

Summing over m

$$\frac{p^2-1}{8}q = ps + \sum \alpha + \sum \beta$$

Now $\sum p - \alpha + \sum \beta = 1 + \ldots + p' = \frac{p^2-1}{8}$ i.e. $\mu p - \sum \alpha + \sum \beta = \frac{p^2-1}{8}$

But $sp + \sum \alpha + \sum \beta = \frac{p^2-1}{8}q$ therefore

$$\frac{p^2-1}{8}(q-1) = p(s-\mu) + 2\sum \alpha$$

$\frac{p^2-1}{8}q - 1$ is even. $2\sum\alpha$ is even therefore $s \equiv \mu \bmod 2$.

By Gauss's Lemma $\left(\frac{q}{p}\right) = (-1)^{\mu}$ therefore $\left(\frac{q}{p}\right) = (-1)^{s}$

Write $t = \sum_{m=1}^{q'}\left[\frac{mp}{q}\right]$, then $\left(\frac{p}{q}\right) = (-1)^{t}$

So S.T.P $s + t = p'q'$

Consider the set of all numbers $qx - py,\ x = 1, 2, \dots p'\ y = 1, 2, \dots q'$

This set contains $p'q'$ numbers. No element in this set is zero.

The number of positive numbers in this set is

$\sum_{x=1}^{p'}\left[\frac{qx}{p}\right] = s$

The number of negative numbers in this set is

$\sum_{y=1}^{q}\left[\frac{py}{q}\right] = t$

Hence the result.

Proof 2 Write $e(\alpha) = e^{2\pi i\alpha}$

Suppose k is a natural number and a is an integer. We define $S(a,k) = \sum_{x=1}^{k} e\left(\frac{ax^2}{k}\right)$. This is called a Gaussian sum.

Theorem A (Proof postponed)

If k is odd

$$S(1,k) = \left\{\begin{array}{ll} k^{\frac{1}{2}} & \text{if } k \equiv 1 \bmod 4 \\ ik^{\frac{1}{2}} & \text{if } k \equiv -1 \bmod 4 \end{array}\right.$$

$S(1,k) = \frac{1}{2}(1+i)(1-i^{3k})k^{\frac{1}{2}}$.

Theorem B **(i)** If p is an odd prime and $(a,\ p)=1$ then $S(a,p) = \left(\frac{a}{p}\right) S(1,p)$

(ii) If $(k_1,k_2)=1$ then $S(a,k_1k_2) = S(ak_1,k_2)S(ak_2,k_1)$

Proof **(i)**

$$S(a,p) = \sum_{x=1}^{p} e\left(\frac{ax^2}{p}\right) = \sum_{n=1}^{p} c(n)e\left(\frac{an}{p}\right)$$

where $c(n)$ is the number of solutions of $x^2 \equiv n \bmod p$.
When $n = p\exists 1$ solution and $1+\left(\frac{n}{p}\right) = 1$.
When $(n,p)=1$ if n is a quadratic residue $\exists$ 2 solutions and $1+\left(\frac{n}{p}\right)=2$
When $(n,p)=1$ if n is a quadratic non-residue $\exists$ no solutions and $1+\left(\frac{n}{p}\right)=0$. Therefore

$$\begin{aligned} S(a,p) &= \sum_{n=1}^{p}\left(1+\left(\frac{n}{p}\right)\right) e\left(\frac{an}{p}\right) \\ &= \sum_{n=1}^{p}\left(\frac{n}{p}\right) e\left(\frac{an}{p}\right) \\ &= \sum_{n=1}^{p-1}\left(\frac{n}{p}\right) e\left(\frac{an}{p}\right) \end{aligned}$$

$\left[\left(\frac{p}{p}\right)=0\right]$
For $\sum_{n=1}^{p} e\left(\frac{an}{p}\right) = \sum_{n=1}^{p} z^n = x\left(\frac{1-z^p}{1-z}\right) = 0$ since $z = e^{\frac{2\pi i a}{p}} \neq 1$ since $(a,p)=1$.
Write $an = m$
$\left(\frac{n}{p}\right) = \left(\frac{a^2n}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{an}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{m}{p}\right)$
If $(a,p)=1$ an n runs through a R.S.R. then $an=m$ runs through an R.S.R. Therefore

$$\sum_{n=1}^{p-1}\frac{n}{p}e\left(\frac{an}{p}\right) = \sum_{m=1}^{p-1}\left(\frac{a}{p}\right)\left(\frac{m}{p}\right)e\left(\frac{m}{p}\right)$$

therefore

$$S(a,p) = \left(\frac{a}{p}\right)\sum_{m=1}^{p-1}\left(\frac{m}{p}\right)e\left(\frac{m}{p}\right)$$

In particular for $a=1$,
$S(1,p) = i\sum_{m=1}^{p-1}\left(\frac{m}{p}\right)e\left(\frac{m}{p}\right)$
Therefore $S(a,p) = \left(\frac{a}{p}\right)S(1,p)$

(ii) Suppose $(k_1\ k_2)=1$
$S(a,k_1k_2) = \sum_{x=1}^{k_1k_2} e\left(\frac{ax^2}{k_1k_2}\right)$
Suppose u runs through C.S.R. mod k_2 and v runs through C.S.R. mod k_1. Then k_1u+k_2v runs through C.S.R. mod k_1k_2. Therefore

$$\begin{aligned} S(a,k_1k_2) &= \sum_{v=1}^{k_1}\sum_{u=1}^{k_2} e\left(\frac{a(k_1u+k_2v)^2}{k_1k_2}\right) \\ &= \sum_{v=1}^{k_1}\sum_{u=1}^{k_2} e\left(\frac{ak_1u^2}{k_2}\right)e\left(\frac{ak_2v^2}{k_1}\right) \\ &= S(ak_2,k_1)S(ak_1,k_2) \end{aligned}$$

Suppose now that $p,\ q$ are distinct odd primes.

Applying theorem B with $a=1$ we have

$$\begin{aligned} S(1,pq) &= S(p,q)S(q,p) \\ S(1,pq) &= \left(\frac{p}{q}\right)S(1,q)\left(\frac{q}{p}\right)S(1,p) \\ \varepsilon_{pq}(pq)^{\frac{1}{2}} &= \left(\frac{p}{q}\right)\varepsilon_q q^{\frac{1}{2}}\left(\frac{q}{p}\right)\varepsilon_p p^{\frac{1}{2}} \end{aligned}$$

where $\varepsilon_k = \begin{cases} 1 & \text{if } k\equiv 1 \bmod 4 \\ i & \text{if } k\equiv -1 \bmod 4 \end{cases}$

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

In connection with theorem A it is easy to prove the result to within a $\pm$ sign as we shall now see.

If $(2a,k)=1$

$$\begin{aligned} |S(a,k)|^2 &= S(a,k)S(-a,k) \\ &= \sum_{x=1}^{k} e\left(\frac{ax^2}{k}\right)\sum_{y=1}^{k} e\left(\frac{-a(x+y)^2}{k}\right) \text{ sum over C.S.R.} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{x=1}^{k}\sum_{y=1}^{k} e\left(-\frac{2axy}{k}\right) e\left(-\frac{ay^2}{k}\right) \\
&= \sum y = 1^k e\left(-\frac{ay^2}{k}\right) \sum_{x=1}^{k} e\left(\frac{-2axy}{k}\right) \\
&= k
\end{aligned}
$$

The inner sum $= k$ if $y = k$ and 0 otherwise.

$$
\begin{aligned}
S(1,p).S(-1,p) &= p \\
\left(\frac{-1}{p}\right)\{S(1,p)\}^2 &= p \\
S(1,p)^2 &= (\varepsilon_p p^{\frac{1}{2}})^2 \\
\text{therefore } S(1,p) &= \pm\varepsilon_p p^{\frac{1}{2}}
\end{aligned}
$$

Corollary to Gauss's Lemma

$$
\left(\frac{2}{o}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if} p \equiv \pm 1\ (8) \\ -1 & \text{if} p \equiv \pm 3\ (8) \end{cases}
$$

Jacobi Symbol We define, for m odd

$$
\left(\frac{n}{m}\right) = \begin{cases} 1 & \text{if } m = \pm 1 \\ \left(\frac{n}{p_1}\right)^{\alpha_1}\left(\frac{n}{p_2}\right)^{\alpha_2}\dots\left(\frac{n}{p_r}\right)^{\alpha_r} & \text{if } m = p_1^{\alpha_1}\dots p_r^{\alpha_r} \end{cases}
$$

Then $\left(\frac{n+km}{m}\right) = \frac{n}{m}\left(\frac{n}{m_1m_2}\right) = \left(\frac{n}{m_1}\right)\left(\frac{n}{m_2}\right)$

$\left(\frac{n_1n_2}{m}\right) = \left(\frac{n_1}{m}\right)\left(\frac{n_2}{m}\right)$

If $x^2 \equiv n \bmod m$ then $\left(\frac{n}{m}\right) = +1$ but the converse is not true.

Theorem (i) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ $m > 0$ m odd.

(ii) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$ m odd.

(iii) $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$

$m,\ n$ odd but not both negative and $(m,\ n) = 1$.

Proof Suppose $n = \prod p;\ m = \prod q\ p \neq q$. Suppose first that $m > 0$ $n > 0$

(i) $\left(\frac{-1}{m}\right)\prod_q\left(\frac{-1}{q}\right) = (-1)^{\sum\frac{q-1}{2}} = (-1)^{Am}$

(ii) $\left(\frac{2}{m}\right) = \prod_q\left(\frac{2}{q}\right) = (-1)^{\sum\frac{q^2-1}{8}} = (-1)^{Bm}$

(iii) $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_{p,\ q}\left\{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\right\} = (-1)^{\sum\frac{p-1}{2}\sum\frac{q-1}{2}} = (-1)^{AnAm}$

So R.T.P. $A_m \equiv \frac{m-1}{2} \bmod 2,\ B_m \equiv \frac{m^2-1}{8} \bmod 2$.

Now $r,\ s$ odd $\Rightarrow (r-1)(s-1) \equiv 0 \bmod 4$.

So $\frac{r-1}{2} + \frac{s-1}{2} \equiv \frac{rs-1}{2} \bmod 2$ and by induction

$\frac{r_1-1}{2} + \ldots + \frac{r_v-1}{2} \equiv \frac{r_1\ldots r_v-1}{2} \bmod 2$

Also $(r^2-1)(s^2-1) \equiv 0 \bmod 64$ and so

$\frac{r^2-1}{8} + \frac{s^2}{8} \equiv \frac{r^2s^2-1}{8} \bmod 8$

and by induction

$\frac{r_1^2-1}{8} + \ldots + \frac{r_v^2-1}{8} = \frac{r_1^2\ldots r_v^2-1}{8}$

Thus $A_m \equiv \frac{m-1}{2} \bmod 2$ and $B_m \equiv \frac{m^2-1}{8} \bmod 8$ and so mod 2.

(i) and (ii) are unaffected by our assumption that $m > 0\ n > 0$.

(iii) Suppose $m > 0\ n < 0$.

Write $n = -n'$

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \left(-\frac{n'}{m}\right)\left(\frac{m}{n'}\right) = \left(-\frac{1}{m}\right)\left(\frac{n'}{m}\right)\left(\frac{m}{n'}\right) = (-1)^{\frac{m-1}{2}+\frac{n'-1}{2}\cdot\frac{m-1}{2}}$$

Now $\left(\frac{m-1}{2}\right) + \left(\frac{n'-1}{2}\right)\left(\frac{m-1}{2}\right) = \left(\frac{m-1}{2}\right)\left(\frac{-n+1}{2}\right) = \left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right) \bmod 2$.

We can use the Jacobi symbol to evaluate Legendre symbols by this theorem.

e.g. $\left(\frac{31}{103}\right) = -\left(\frac{103}{31}\right) = -\left(-\frac{21}{31}\right) = \left(\frac{31}{-21}\right) = \left(\frac{31}{21}\right) = \left(\frac{-11}{-21}\right) = \left(\frac{21}{11}\right) = \left(\frac{-1}{11}\right) = -1$

Exercise (1) p an odd prime. Consider $1, 2, 3\ldots$. Pick the least quadratic non-residue q mod p. Prove $q = O(p^{\frac{1}{2}})$

It is known that $q = O(p^\alpha)\ \alpha > \frac{1}{4}e^{-\frac{1}{2}}$

It is conjectured that $q = O(p^\varepsilon)$

[Hint q must be prime. $\exists$ a multiple of q such that $p < mq < p + q$. What about m]

(2) $1, 2, \ldots p-1\ \varepsilon_1 = \pm 1\ \varepsilon_2 = \pm 1$

For how many n among $1, 2, \ldots p-2$ is $\left(\frac{n}{p}\right) = \varepsilon_1$ $\left(\frac{n+1}{p}\right) = \varepsilon_2$

Suppose the answer is $\psi(\varepsilon_1, \varepsilon_2)$

$4\psi(\varepsilon_1, \varepsilon_2) = \sum_{n=1}^{p-2} \left(1 + \varepsilon_1 \left(\frac{n}{p}\right)\right) \left(1 + \varepsilon_2 \left(\frac{n+1}{p}\right)\right)$