Definition. Let p be a prime and let $(a,p)=1$. If the congruence $x^2 \equiv a \pmod{p}$ has an integer solution, then we say that a is a *quadratic residue* modulo p; if not, then a is a *quadratic non-residue* modulo p.

The following result has been obtained earlier (without the language of quadratic residues):

Proposition 1 (Euler's Criterion)**.** *Let p be an odd prime and let $(a,p)=1$. Then, a is a quadratic residue mod p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.*

Question: if $a^{(p-1)/2} \not\equiv 1 \pmod{p}$, then $a^{(p-1)/2} \equiv ??? \pmod{p}$?

We mention without proof, the following fact:

Proposition 2. *The multiplicative group of the nonzero elements of $\mathbb{Z}_p$ (under multiplication mod p) is cyclic.*

Any generator of this group is called a *primitive element* mod p.

Corollary 3. *Let g be a primitive element modulo an odd prime p. Then, g^r is a quadratic residue mod p if and only if r is even.*

Definition. For any odd prime p and any $a \in \mathbb{Z}$, the *Legendre symbol* $(\frac{a}{p})$ is defined as follows: $(\frac{a}{p})=1$ if a is a quadratic residue mod p, $(\frac{a}{p})=0$ if $p|a$, and $(\frac{a}{p})=-1$ if a is a quadratic non-residue mod p.

Exercise 1. Let p be an odd prime. Prove the following:
(i) $(\frac{a}{p})=(\frac{b}{p})$ if $a \equiv b \pmod{p}$, (ii) $(\frac{ab}{p})=(\frac{a}{p})(\frac{b}{p})$, (iii) $a^{(p-1)/2} \equiv (\frac{a}{p}) \pmod{p}$.

An important and, at the same time, amazing way of determining the Legendre symbol was suggested by Gauss. For any $n \in \mathbb{Z}$ and any odd prime p, define the *least residue of n modulo p* to be the unique integer r between $-(p-1)/2$ and $(p-1)/2$ such that $n \equiv r \pmod{p}$. Notation: $r=\rho_p(n)$.

Proposition 4 (Gauss' Lemma)**.** *Let p be an odd prime and let $(a,p)=1$. Let α be the number of integers j, $1 \le j \le (p-1)/2$, such that $\rho_p(ja)<0$. Then, $(\frac{a}{p})=(-1)^\alpha$.*

Proof. For any j such that $1 \le j \le (p-1)/2$, we have $ja \equiv \rho_p(ja) = \operatorname{sgn}(\rho_p(ja))|\rho_p(ja)| \pmod{p}$. Since $1 \le |\rho_p(ja)| \le (p-1)/2$ and the numbers ja are pairwise incongruent mod p, we see that as j takes the integral values in $[1,(p-1)/2]$, so does the quantity $|\rho_p(ja)|$. Therefore, multiplying through the above congruences yields

$$((p-1)/2)!a^{(p-1)/2} = \prod_j (ja) \equiv \prod_j \operatorname{sgn}(\rho_p(ja)) \prod_j |\rho_p(ja)| = \prod_j \operatorname{sgn}(\rho_p(ja)) \cdot ((p-1)/2)! \pmod{p}.$$

Cancelling the factor $((p-1)/2)!$ and using the definition of α finally gives $(\frac{a}{p}) \equiv a^{(p-1)/2} \equiv \prod_j \operatorname{sgn}(\rho_p(ja)) = (-1)^\alpha \pmod{p}$. □

Exercise 2. Let p be an odd prime. Use Gauss' Lemma to calculate $(\frac{2}{p})$ (i.e. use it to answer the question: for which odd primes p is 2 a square modulo p?). Look at the cases $p=17,19,23,29$ for inspiration, if needed.

Exercise 3. Show that if p is an odd prime and a is an *odd* integer such that $(a,p)=1$, then $(\frac{a}{p})=(-1)^\beta$ where $\beta = \sum_{1 \le j \le (p-1)/2} \lfloor ja/p \rfloor$.

Exercise 4. Let p be an odd prime. Prove that (i) $(\frac{-1}{p})=(-1)^{(p-1)/2}$, (ii) $(\frac{2}{p})=(-1)^{(p^2-1)/8}$, (iii) $(\frac{3}{p})=1$ if $p \equiv \pm 1 \pmod{12}$ and $(\frac{3}{p})=-1$ if $p \equiv \pm 5 \pmod{12}$.

GAP Commands:

```
Legendre(a,p)
```