Let us suppose, for example, that p is a prime which is $\equiv 3$ *mod* 4. There is a nice way to think of the field $\mathbf{F}_{p^2}$ which generalizes to other situations. Let R denote the Gaussian integer ring (see Exercise 14 of § I.2). Sometimes we write $R = \mathbf{Z}+\mathbf{Z}i$, meaning the set of all integer combinations of 1 and i. If m is any Gaussian integer, and $\alpha = a + bi$ and $\beta = c + di$ are two Gaussian integers, we write $\alpha \equiv \beta \ mod\ m$ if $\alpha - \beta$ is divisible by m, i.e., if the quotient is a Gaussian integer. We can then look at the set R/mR of residue classes modulo m; just as in the case of ordinary integers, residue classes can be added or multiplied, and the residue class of the result does not depend on which representatives were chosen for the residue class factors. Now if $m = p + 0i$ is a prime number which is $\equiv 3$ *mod* 4, it is not hard to show that R/pR is the field $\mathbf{F}_{p^2}$.

Quadratic residues. Suppose that p is an odd prime, i.e., $p > 2$. We are interested in knowing which of the nonzero elements $\{1, 2, \ldots, p-1\}$ of $\mathbf{F}_p$ are squares. If some $a \in \mathbf{F}_p^*$ is a square, say $b^2 = a$, then a has precisely two square roots $\pm b$ (since the equation $X^2 - a = 0$ has at most two solutions in a field). Thus, the squares in $\mathbf{F}_p^*$ can all be found by computing $b^2 \ mod\ p$ for $b = 1, 2, 3, \ldots, (p-1)/2$ (since the remaining integers up to $p - 1$ are all $\equiv -b$ for one of these b), and precisely half of the elements in $\mathbf{F}_p^*$ are squares. For example, the squares in $\mathbf{F}_{11}$ are $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 5$, and $5^2 = 3$. The squares in $\mathbf{F}_p$ are called *quadratic residues* modulo p. The remaining nonzero elements are called *nonresidues*. For $p = 11$ the nonresidues are 2, 6, 7, 8, 10. There are $(p-1)/2$ residues and $(p-1)/2$ nonresidues.

If g is a generator of $\mathbf{F}_p$, then any element can be written in the form g^j. Thus, the square of any element is of the form g^j with j even. Conversely, any element of the form g^j with j even is the square of some element, namely $\pm g^{j/2}$.

The Legendre symbol. Let a be an integer and $p > 2$ a prime. We define the *Legendre symbol* $\left(\frac{a}{p}\right)$ to equal 0, 1 or -1, as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a; \\ 1, & \text{if } a \text{ is a quadratic residue } mod\ p; \\ -1, & \text{if } a \text{ is a nonresidue } mod\ p. \end{cases}$$

Thus, the Legendre symbol is simply a way of identifying whether or not an integer is a quadratic residue modulo p.

Proposition II.2.2.

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \ mod\ p.$$

Proof. If a is divisible by p, then both sides are $\equiv 0 \ mod\ p$. Suppose $p \not| a$. By Fermat's Little Theorem, in $\mathbf{F}_p$ the square of $a^{(p-1)/2}$ is 1, so $a^{(p-1)/2}$ itself is ± 1. Let g be a generator of $\mathbf{F}_p^*$, and let $a = g^j$. As we saw, a is a residue if and only if j is even. And $a^{(p-1)/2} = g^{j(p-1)/2}$ is 1 if and