only if $j(p-1)/2$ is divisible by $p-1$, i.e., if and only if j is even. Thus, both sides of the congruence in the proposition are ± 1 in $\mathbf{F}_p$, and each side is $+1$ if and only if j is even. This completes the proof.

Proposition II.2.3. *The Legendre symbol satisfies the following properties:*

(a) $(\frac{a}{p})$ *depends only on the residue of* a *modulo* p*;*

(b) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$*;*

(c) *for* b *prime to* p, $(\frac{ab^2}{p}) = (\frac{a}{p})$*;*

(d) $(\frac{1}{p}) = 1$ *and* $(\frac{-1}{p}) = (-1)^{(p-1)/2}$.

Proof. Part (a) is obvious from the definition. Part (b) follows from Proposition II.2.2, because the right side is congruent modulo p to $a^{(p-1)/2}\cdot b^{(p-1)/2} = (ab)^{(p-1)/2}$, as is the left side. Part (c) follows immediately from part (b). The first equality in part (d) is obvious, because $1^2 = 1$, and the second equality comes from Corollary 2 of Proposition II.2.1 (or by taking $a = -1$ in Proposition II.2.2). This completes the proof.

Part (b) of Proposition II.2.3 shows that one can determine if a number a is a quadratic residue modulo p, i.e., one can evaluate $(\frac{a}{p})$, if one factors a and knows the Legendre symbol for the factors. The first step in doing this is to write a as a power of 2 times an odd number. We then want to know how to evaluate $(\frac{2}{p})$.

Proposition II.2.4.

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

Proof. Let $f(n) = (-1)^{(n^2-1)/8}$ for n odd, $f(n) = 0$ for n even. We want to show that $(\frac{2}{p}) = f(p)$. Of the various ways of proving this, we shall use an efficient method based on what we already know about finite fields. Since $p^2 \equiv 1 \bmod 8$ for any odd prime p, we know that the field $\mathbf{F}_{p^2}$ contains a primitive 8-th root of unity. Let $\xi \in \mathbf{F}_{p^2}$ denote a primitive 8-th root of 1. Note that $\xi^4 = -1$. Define $G = \sum_{j=0}^{7} f(j)\xi^j$. ($G$ is an example of what is called a *Gauss sum.*) Then $G = \xi - \xi^3 - \xi^5 + \xi^7 = 2(\xi - \xi^3)$ (because $\xi^5 = \xi^4\xi = -\xi$ and $\xi^7 = -\xi^3$), and $G^2 = 4(\xi^2 - 2\xi^4 + \xi^6) = 8$. Thus, in $\mathbf{F}_{p^2}$ we have

$$G^p = (G^2)^{(p-1)/2}G = 8^{(p-1)/2}G = \left(\frac{8}{p}\right)G = \left(\frac{2}{p}\right)G,$$

by Proposition II.2.2 and Proposition II.2.3(c). On the other hand, using the definition of G, the fact that $(a+b)^p = a^p + b^p$ in $\mathbf{F}_{p^2}$, and the obvious observation that $f(j)^p = f(j)$, we compute: $G^p = \sum_{j=0}^{7} f(j)\xi^{pj}$. Notice that $f(j) = f(p)f(pj)$, as we easily check. Then, making the change of variables $j' = pj$ (i.e., modulo 8 we have j' running through $0, \ldots, 7$ when j does), we obtain: