$$G^p = \sum_{j=0}^{7} f(p)f(pj)\xi^{pj} = f(p)\sum_{j'=0}^{7} f(j')\xi^{j'} = f(p)G.$$

Comparing the two equalities for G^p gives the desired result. (Notice that we can divide by G, since it is not 0 in $\mathbf{F}_{p^2}$, as is clear from the fact that its square is 8.)

Next, we must deal with the odd prime factors of a. Let q stand for such an odd prime factor. **Warning:** for the remainder of this section, q will stand for an odd prime distinct from p, *not* for a power of p as in the last section.

Since a can be assumed to be smaller than p (by part (a) of Proposition II.2.3), the prime factors q will be smaller than p. The next proposition — the fundamental Law of Quadratic Reciprocity — tells us how to relate $(\frac{q}{p})$ to $(\frac{p}{q})$. The latter Legendre symbol will be easier to evaluate, since we can immediately replace p by its least positive residue modulo q, thereby reducing ourselves to a Legendre symbol involving smaller numbers. The quadratic reciprocity law states that $(\frac{q}{p})$ and $(\frac{p}{q})$ are the same unless p and q are both $\equiv 3$ *mod* 4, in which case they are the negatives of one another. This can be expressed as a formula using the fact that $(p-1)(q-1)/4$ is even unless both primes are $\equiv 3$ *mod* 4, in which case it is odd.

Proposition II.2.5 (Law of Quadratic Reciprocity). *Let p and q be two odd primes. Then*

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \ mod\ 4; \\ \left(\frac{p}{q}\right) & \text{otherwise.} \end{cases}$$

Proof. There are several dozen proofs of quadratic reciprocity in print. We shall give a particularly short proof along the lines of the proof of the last proposition, using finite fields. Let f be any power of p such that $p^f \equiv 1$ *mod* q. For example, we can always take $f = q - 1$. Then, as we saw at the beginning of the section (Proposition II.2.1), the field $\mathbf{F}_{p^f}$ contains a primitive q-th root of unity, which we denote ξ. (Remember that q here denotes another prime besides p; it does *not* denote p^f.) We define the "Gauss sum" G by the formula $G = \sum_{j=0}^{q-1}(\frac{j}{q})\xi^j$. In the next paragraph we shall prove that $G^2 = (-1)^{(q-1)/2}q$. Before proving that lemma, we show how to use it to prove our proposition. The proof is very similar to the proof of Proposition II.2.4. We first obtain (using the lemma to be proved below):

$$\begin{aligned} G^p &= (G^2)^{(p-1)/2}G = \left((-1)^{(q-1)/2}q\right)^{(p-1)/2}G \\ &= (-1)^{(p-1)(q-1)/4}q^{(p-1)/2}G = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)G, \end{aligned}$$

by Proposition II.2.2 with a replaced by q (recall that we're working in a field of characteristic p, namely $\mathbf{F}_{p^f}$, and so congruence modulo p becomes