can suppose that $g.c.d.(m, n) = 1$. Next, we write $m$ and $n$ as products of primes: $m = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$. (The $p$'s and $q$'s include repetitions if $m$ or $n$ has a square factor.) In converting from $(\frac{m}{n}) = \prod_{i,j}(\frac{p_i}{q_j})$ to $(\frac{n}{m}) = \prod_{i,j}(\frac{q_j}{p_i})$ we must apply the quadratic reciprocity law for the Legendre symbol $rs$ times. The number of $(-1)$'s we get is the number of times both $p_i$ and $q_j$ are $\equiv 3 \ mod\ 4$, i.e., it is the product of the number of primes $\equiv 3 \ mod\ 4$ in the factorization of $m$ and in the factorization of $n$. Thus, $(\frac{m}{n}) = (\frac{n}{m})$ unless there are an odd number of primes $\equiv 3 \ mod\ 4$ in both factorizations, in which case $(\frac{m}{n}) = -(\frac{n}{m})$. But a product of odd primes, such as $m$ or $n$, is $\equiv 3 \ mod\ 4$ if and only if it contains an odd number of primes which are $\equiv 3 \ mod\ 4$. We conclude that $(\frac{m}{n}) = (\frac{n}{m})$ unless both $m$ and $n$ are $\equiv 3 \ mod\ 4$, as was to be proved. This gives us the reciprocity law for the Jacobi symbol.

**Example 2.** We return to Example 1, and show how to evaluate the Legendre symbol without factoring 1872, except to take out the power of 2. By the reciprocity law for the Jacobi symbol we have

$$-\left(\frac{1872}{7411}\right) = -\left(\frac{16}{7411}\right)\left(\frac{117}{7411}\right) = -\left(\frac{7411}{117}\right) = -\left(\frac{40}{117}\right),$$

and this is equal to $-(\frac{2}{117})(\frac{5}{117}) = (\frac{5}{117}) = (\frac{117}{5}) = (\frac{2}{5}) = -1$.

**Square roots modulo *p*.** Using quadratic reciprocity, one can quickly determine whether or not an integer $a$ is a quadratic residue modulo $p$. However, if it is a residue, that does not tell us how to find a solution to the congruence $x^2 \equiv a \ mod\ p$ — it tells us only that a solution exists. We conclude this section by giving an algorithm for finding a square root of a residue $a$ once we know any *non*residue $n$.

Kannst
[illegible]
[illegible]

Let $p$ be an odd prime, and suppose that we somehow know a quadratic nonresidue $n$. Let $a$ be an integer such that $(\frac{a}{p}) = 1$. We want to find an integer $x$ such that $x^2 \equiv a \ mod\ p$. Here is how we proceed. First write $p - 1$ in the form $2^\alpha \cdot s$, where $s$ is odd. Then compute $n^s$ modulo $p$, and call that $b$. Next compute $a^{(s+1)/2}$ modulo $p$, and call that $r$. Our first claim is that $r$ comes reasonably close to being a square root of $a$. More precisely, if we take the ratio of $r^2$ to $a$, we claim that we get a $2^{\alpha-1}$-th root of unity modulo $p$. Namely, we compute (for brevity, we shall use equality to mean congruence modulo $p$, and we use $a^{-1}$ to mean the inverse of $a$ modulo $p$):

$$(a^{-1}r^2)^{2^{\alpha-1}} = a^{s2^{\alpha-1}} = a^{(p-1)/2} = \left(\frac{a}{p}\right) = 1.$$

We must then modify $r$ by a suitable $2^\alpha$-th root of unity to get an $x$ such that $x^2/a$ is 1. To do this, we claim that $b$ is a *primitive* $2^\alpha$-th root of unity, which means that all $2^\alpha$-th roots of unity are powers of $b$. To see this, first we note that $b$ is a $2^\alpha$-th root of 1, because $b^{2^\alpha} = n^{2^\alpha s} = n^{p-1} = 1$. If $b$ weren't primitive, there would be a lower power (a divisor of $2^\alpha$) of $b$ that gives 1. But then $b$ would be an even power of a primitive $2^\alpha$-th root of unity, and so would be a square in $\mathbf{F}_p^*$. This is impossible, because $(\frac{b}{p}) = (\frac{n}{p})^s = -1$ (since $s$ is odd and $n$ is a nonresidue). Thus, $b$ is a primitive $2^\alpha$-th root of unity. So it remains to find a suitable power $b^j$, $0 \le j < 2^\alpha$, such that $x = b^j r$ gives the desired square root of $a$. To do that, we write $j$ in binary as $j = j_0 + 2j_1 + 4j_2 + \cdots + 2^{\alpha-2}j_{\alpha-2}$, and show how one successively determines whether $j_0, j_1, \ldots$ is 0 or 1. (Note that we may suppose that $j < 2^{\alpha-1}$, since $b^{2^{\alpha-1}} = -1$, and so $j$ can be modified by $2^{\alpha-1}$ to give another $j$ for which $b^j r$ is the other square root of $a$.) Here is the inductive procedure for determining the binary digits of $j$:

1. Raise $(r^2/a)$ to the $2^{\alpha-2}$-th power. We proved that the square of this is 1. Hence, you get either ±1. If you get 1, take $j_0 = 0$; if you get $-1$, take $j_0 = 1$. Notice that $j_0$ has been chosen so that $((b^{j_0}r)^2/a)$ is a $2^{\alpha-2}$-th root of unity.

2. Suppose you've found $j_0, \ldots, j_{k-1}$ such that $(b^{j_0+2j_1+\cdots+2^{k-1}j_{k-1}}r)^2/a$ is a $2^{\alpha-k-1}$-th root of unity, and you want to find $j_k$. Raise this number to half the power that gives 1, and choose $j_k$ according to whether you get $+1$ or $-1$:

$$\text{if} \qquad \left(\frac{\left(b^{j_0+2j_1+\cdots+2^{k-1}j_{k-1}}r\right)^2}{a}\right)^{2^{\alpha-k-2}} = \begin{cases} 1 \\ -1 \end{cases},$$

$$\text{then take} \qquad j_k = \begin{cases} 0 \\ 1 \end{cases}, \quad \text{respectively.}$$

We easily check that with this choice of $j_k$ the "corrected" value comes closer to being a square root of $a$, i.e., we find that $(b^{j_0+2j_1+\cdots+2^k j_k}r)^2/a$ is a $2^{\alpha-k-2}$-th root of unity.

When we get to $k = \alpha - 2$ and find $j_{\alpha-2}$, we then have

$$(b^{j_0+2j_1+\cdots+2^{\alpha-2}j_{\alpha-2}}r)^2/a = 1,$$

i.e., $b^j r$ is a square root of $a$, as desired.

**Example 3.** Use the above algorithm to find a square root of $a = 186$ modulo $p = 401$.

**Solution.** The first nonresidue is $n = 3$. We have $p - 1 = 2^4 \cdot 25$, and so $b = 3^{25} = 268$ and $r = a^{13} = 103$ (where we use equality to denote congruence modulo $p$). After first computing $a^{-1} = 235$, we note that $r^2/a = 98$, which must