

**Example 1.** Determine whether 7411 is a residue modulo the prime 9283.

**Solution.** Since 7411 and 9283 are both primes which are  $\equiv 3 \pmod{4}$ , we have  $\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right) = -\left(\frac{1872}{7411}\right)$  by part (a) of Proposition II.2.3. Since  $1872 = 2^4 \cdot 3^2 \cdot 13$ , by part (c) of Proposition II.2.3 we find that the desired Legendre symbol is  $-\left(\frac{13}{7411}\right)$ . But we can now apply quadratic reciprocity again: since  $13 \equiv 1 \pmod{4}$  we find that  $-\left(\frac{13}{7411}\right) = -\left(\frac{7411}{13}\right) = -\left(\frac{1}{13}\right) = -1$ . In other words, 7411 is a quadratic nonresidue.

One difficulty with this method of evaluating Legendre symbols is that at each stage we must factor the number on top in order to apply Proposition II.2.5. If our numbers are astronomically large, this will be very time-consuming. Fortunately, it is possible to avoid any need for factoring (except taking out powers of 2, which is very easy), once we prove a generalization of the quadratic reciprocity law that applies to all positive odd integers, not necessarily prime. But we first need a definition which generalizes the definition of the Legendre symbol.

**The Jacobi symbol.** Let  $a$  be an integer, and let  $n$  be any positive odd number. Let  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  be the prime factorization of  $n$ . Then we define the *Jacobi symbol*  $\left(\frac{a}{n}\right)$  as the product of the Legendre symbols for the prime factors of  $n$ :

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

A word of warning is in order here. If  $\left(\frac{a}{n}\right) = 1$  for  $n$  composite, it is *not* necessarily true that  $a$  is a square modulo  $n$ . For example,  $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$ , but there is no integer  $x$  such that  $x^2 \equiv 2 \pmod{15}$ .

We now generalize Propositions II.2.4–5 to the Jacobi symbol.

**Proposition II.2.6.** *For any positive odd  $n$  we have  $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$ .*

**Proof.** Let  $f(n)$  denote the function on the right side of the equality, as in the proof of Proposition II.2.4. It is easy to see that  $f(n_1 n_2) = f(n_1)f(n_2)$  for any two odd numbers  $n_1$  and  $n_2$ . (Just consider the different possibilities for  $n_1$  and  $n_2$  modulo 8.) This means that the right side of the equality in the proposition equals  $f(p_1)^{\alpha_1} \cdots f(p_r)^{\alpha_r} = \left(\frac{2}{p_1}\right)^{\alpha_1} \cdots \left(\frac{2}{p_r}\right)^{\alpha_r}$  by Proposition II.2.4. But this is  $\left(\frac{2}{n}\right)$ , by definition.

**Proposition II.2.7.** *For any two positive odd integers  $m$  and  $n$  we have  $\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4} \left(\frac{n}{m}\right)$ .*

**Proof.** First note that if  $m$  and  $n$  have a common factor, then it follows from the definition of the Legendre and Jacobi symbols that both sides are zero. So we can suppose that  $\text{g.c.d.}(m, n) = 1$ . 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  $\left(\frac{m}{n}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right)$  to  $\left(\frac{n}{m}\right) = \prod_{i,j} \left(\frac{q_j}{p_i}\right)$  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  $\equiv 3 \pmod{4}$ , i.e., it is the product of the number of primes  $\equiv 3 \pmod{4}$  in the factorization of  $m$  and in the factorization of  $n$ . Thus,  $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$  unless there are an odd number of