NUMBER THEORY NOTES ON JACOBI SYMBOLS
Vanderbilt University, Spring 2023

We have seen that Legendre symbols like $\left(\frac{a}{p}\right)$, which are defined only when the bottom is a prime, determine whether or not a is a quadratic residue mod p. We have also seen that the special formulas for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$, together with quadratic reciprocity and the periodicity property of the Legendre symbols, gives a way to compute these symbols in many cases. For instance, if we wish to know if 3 is a residue modulo 97, we can compute:

$$\left(\frac{3}{97}\right) = (-1)^{1\cdot 48}\left(\frac{97}{3}\right) = \left(\frac{1}{3}\right) = 1,$$

where we used that $97 \equiv 1 \pmod 3$ and that 1 is a square modulo 3 as it is a square just in $\mathbb{Z}$. As another example, using multiplicativity of the symbol as a function of the top, and that $880 = 2^4 \cdot 5 \cdot 11$,

$$\begin{aligned}\left(\frac{880}{863}\right) &= \left(\frac{2}{863}\right)^4\left(\frac{5}{863}\right)\left(\frac{11}{863}\right) = -\left(\frac{863}{5}\right)\cdot\left(\frac{863}{11}\right) = -\left(\frac{3}{5}\right)\left(\frac{5}{11}\right)\\ &= -\left(\frac{5}{3}\right)\left(\frac{11}{5}\right) = -\left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = -(-1)\cdot 1 = 1.\end{aligned}$$

Note that when using the prime factorizations that square factors come out in the wash as even powers of ± 1 are always $+1$. Of course, the 880 could have been reduced modulo 863 first, but this example was included to illustrate that although the method of factoring, flipping with reciprocity, and using the special formulas to get rid of 2's and -1's if needed always works, there are two parts that make it computationally difficult. One is that factoring into primes is actually very difficult, and the second is that usually there will be a number of prime factorizations, making it necessary to compute many symbols.

There is a notational tool, invented by Jacobi, which helps ease these computations, even when the bottom number is a prime, by exptending the bottom to more general numbers.

Definition. If n is an odd positive integer whose prime factorization is $n = p_1^{t_1} \cdot \ldots \cdot p_m^{t_m}$, then we define the **Jacobi symbol** for any $(a, n) = 1$ to be

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{t_1} \cdot \ldots \cdot \left(\frac{a}{p_m}\right)^{t_m}.$$

This symbol is extended to be defined for all integers a by declaring that $\left(\frac{a}{p}\right) = 0$ if $(a, n) > 1$.

Essentially, using our ideas from Chapter 3, the point is that this is the unique extension to odd integers n which is completely multiplicative as a function of the bottom argument. It is important to note here that the symbol $\left(\frac{a}{n}\right)$ is not simply 1 iff a is a quadratic residue modulo n; we'll skip the exact characterization, but think of this definition as a computational tool. The Jacobi symbol satisfies the following basic properties.

Theorem. *Assuming the notation above, the following are true.*

1. *If $a \equiv b \pmod n$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$. That is, as a function of the top, the Jacobi symbol is periodic modulo n.*
2. *For any a, b, we have $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$. That is, the Jacobi symbol is a completely multiplicative function of the top argument.*
3. *For any m, n, we have $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{n}\right)$. That is, the Jacobi symbol is a completely multiplicative function of the bottom argument.*
4. *We have $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.*
5. *We have $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.*
6. *We have the following quadratic reciprocity law, where m and n are odd, coprime, positive integers:*
$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\left(\frac{m-1}{2}\right)\cdot\left(\frac{n-1}{2}\right)}.$$

Proof. Throughout the proof, we will write the prime factorization of n as $n = p_1^{t_1} \cdot \ldots \cdot p_m^{t_m}$.

(1) For any prime $p|n$, if $a \equiv b \pmod{n}$, then $a \equiv b \pmod{p}$, and so by the equivalent property for Legendre symbols, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Thus,

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{t_i} = \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{t_i} = \left(\frac{b}{n}\right).$$

(2) Each factor in the Jacobi symbol, of typical form $\left(\frac{ab}{p_i}\right)^{t_i}$, splits up as $\left(\frac{a}{p_i}\right)^{t_i}\left(\frac{b}{p_i}\right)^{t_i}$ due to the complete multiplicativity of the Legendre symbol. Thus, the same is true for the Jacobi symbol which is the product of all these terms.

(3) The Jacobi symbol is defined so that this property holds; that is, it is defined through the prime factorization of the bottom argument, so this multiplicativity relation is automatic.

(4) For each prime p, using the special formula $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, we find

$$\left(\frac{-1}{n}\right) = \prod_{i=1}^{m} \left(\frac{-1}{p_i}\right)^{t_i} = (-1)^{\sum_{i=1}^{m} t_i\left(\frac{p_i-1}{2}\right)}.$$

We now write

$$n = \prod_{i=1}^{m} p_i^{t_i} = \prod_{i=1}^{m} \left(1 + (p_i - 1)\right)^{t_i}.$$

Since each prime p_i is odd (recall that n is odd), each term $p_i - 1$ is even, and so by using the binomial expansion formula on $(1 + (p_i - 1))^{t_i}$, we see that

$$(1 + (p_i - 1))^{t_i} \equiv 1 + t_i(p_i - 1) \pmod{4}.$$

Using the same parity argument, the product of any two typical terms as on the right hand side of this congruence expands as

$$(1 + t_i(p_i - 1))\,(1 + t_j(p_j - 1)) \equiv 1 + t_i(p_i - 1) + t_j(p_j - 1) \pmod{4}.$$

Thus, plugging these congruences into the above formula for factorizing n, we find that

$$n \equiv 1 + \sum_{i=1}^{m} t_i(p_i - 1) \pmod{4},$$

and hence

$$\frac{n-1}{2} \equiv \sum_{i=1}^{m} t_i \left(\frac{p_i - 1}{2}\right) \pmod{2}.$$

By combining with the first formula for $\left(\frac{-1}{n}\right)$ above, we find $\left(\frac{-1}{b}\right) = (-1)^{\frac{n-1}{2}}$, as desired.

(5) For odd primes p, we know that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, and so

$$\left(\frac{2}{n}\right) = \prod_{i=1}^{m} \left(\frac{2}{p_i}\right)^{t_i} = (-1)^{\sum_{i=1}^{m} t_i\left(\frac{p_i^2-1}{8}\right)}.$$

Similar to the argument in the proof of (4),

$$n^2 = \prod_{i=1}^{m} \left(1 + (p_i^2 - 1)\right)^{t_i}.$$

Since each p_i is odd, each term $p_i^2 - 1$ is 0 modulo 8. Thus, by the binomial theorem again, we find that

$$(1 + (p_i^2 - 1))^{t_i} \equiv 1 + t_i(p_i^2 - 1) \pmod{64},$$

and a product of two typical factors becomes

$$\left(1+t_i(p_i^2-1)\right)\left(1+t_j(p_j^2-1)\right) \equiv 1+t_i(p_i^2-1)+t_j(p_j^2-1) \pmod{64}.$$

Thus, $n^2 \equiv 1+\sum_{i=1}^m t_i(p_i^2-1) \pmod{64}$, and so

$$\frac{n^2-1}{8} \equiv \sum_{i=1}^m t_i\left(\frac{p_i^2-1}{8}\right) \pmod 8.$$

Combining with the formula for $\left(\frac{2}{n}\right)$ above, we have found the desired

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

(6) Factor m and n into prime powers:

$$m = \prod_{i=1}^s p_i^{a_i},$$

$$n = \prod_{i=1}^r q_i^{b_i}.$$

By definition of the Jacobi symbol and complete multiplicativity of the Legendre symbol,

$$\left(\frac{m}{n}\right) = \prod_{i=1}^r \left(\frac{m}{q_i}\right)^{b_i} = \prod_{i=1}^r \prod_{j=1}^s \left(\frac{p_j}{q_i}\right)^{b_i a_j}.$$

Similarly,

$$\left(\frac{n}{m}\right) = \prod_{j=1}^s \prod_{i=1}^r \left(\frac{q_i}{p_j}\right)^{a_j b_i}.$$

Thus,

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^r \prod_{j=1}^s \left(\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right)\right)^{a_j b_i},$$

which by quadratic reciprocity for odd distinct primes becomes

$$\prod_{i=1}^r \prod_{j=1}^s (-1)^{\left(a_j\left(\frac{p_j-1}{2}\right)\right)\left(b_i\left(\frac{q_i-1}{2}\right)\right)} = (-1)^{\sum_{i=1}^r \sum_{j=1}^s \left(a_j\left(\frac{p_j-1}{2}\right)\right)\left(b_i\left(\frac{q_i-1}{2}\right)\right)} = (-1)^{\left(\sum_{j=1}^s a_j\left(\frac{p_j-1}{2}\right)\right)\cdot\left(\sum_{i=1}^r b_i\left(\frac{q_i-1}{2}\right)\right)}$$

We have showed in the above parts of the proof of this theorem that $\sum_{j=1}^s a_j\left(\frac{p_j-1}{2}\right) \equiv \frac{m-1}{2} \pmod 2$, and similarly for n. Thus, this last expression is equal to $(-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)}$, as the exponents are all congruent modulo 2.

□

To illustrate the power of Jacobi's symbol, we give a numerical example.

Example. We will compute $\left(\frac{713}{1009}\right)$. Note that 1009 is a prime.

Method 1: Slow way, only using Legendre symbols We first factor $713 = 23 \cdot 31$ (this is already not so fast to compute by hand). Thus,

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right).$$

Since $(1009-1)/2$ is even, when we flip both symbols with reciprocity, we will get no minus signs, and so this becomes

$$\left(\frac{1009}{23}\right)\left(\frac{1009}{31}\right).$$

Reducing modulo the bottom, we obtain

$$\left(\frac{20}{23}\right)\left(\frac{17}{31}\right).$$

Factoring the tops into primes again gives

$$\left(\frac{2}{23}\right)^2\left(\frac{5}{23}\right)\left(\frac{17}{31}\right)=\left(\frac{5}{23}\right)\left(\frac{17}{31}\right).$$

Flipping with reciprocity again yields

$$\left(\frac{23}{5}\right)(-1)^{(\frac{23-1}{2})(\frac{5-1}{2})}\left(\frac{31}{17}\right)(-1)^{(\frac{31-1}{2})(\frac{17-1}{2})}=\left(\frac{23}{5}\right)\left(\frac{31}{17}\right).$$

Reducing the tops mod the bottoms again gives

$$\left(\frac{3}{5}\right)\left(\frac{14}{17}\right),$$

and factoring into primes and using the special formula when 2 is on top gives

$$\left(\frac{3}{5}\right)\left(\frac{2}{17}\right)\left(\frac{7}{17}\right)=\left(\frac{3}{5}\right)\left(\frac{7}{17}\right).$$

Using quadratic reciprocity again gives (note that no sign shows up in the flip as long as at least one of the arguments is $1 \pmod 4$)

$$\left(\frac{5}{3}\right)\left(\frac{17}{7}\right),$$

and reducing the tops mod the bottoms gives

$$\left(\frac{2}{3}\right)\left(\frac{3}{7}\right)=-\left(\frac{3}{7}\right).$$

Using quadratic reciprocity yet again, one obtains

$$\left(\frac{7}{3}\right)=\left(\frac{1}{3}\right)=+1.$$

This is quite tedious indeed when all details are performed, and now we want to see why Jacobi symbols, and the full quadratic reciprocity and special formulas for -1 and 2 as the top argument make life much easier.

Method 2: Fast way using Jacobi symbols and full quadratic reciprocity Note that 1009 is $1 \pmod 4$, so when we use quadratic reciprocity, there is no sign picked up, and hence

$$\left(\frac{713}{1009}\right)=\left(\frac{1009}{713}\right)=\left(\frac{296}{713}\right).$$

We aren't allowed to use the quadratic reciprocity formula for even numbers, so we do need to factor out the 2's, but we do not need to do the full prime factorization of the top. We factor out a 2^3 from the top to get

$$\left(\frac{2}{713}\right)^3\left(\frac{37}{713}\right)=\left(\frac{2}{713}\right)\left(\frac{37}{713}\right).$$

Using the rule for when the top argument is 2, and flipping with reciprocity again (note that 37 is 1 (mod 4)), this becomes

$$\left(\frac{713}{37}\right) = \left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right).$$

Using the rule where the top is 2 and the reciprocity formula one more time, this gives

$$-\left(\frac{37}{5}\right) = -\left(\frac{2}{5}\right) = 1.$$

This agrees with the result obtained in method 1, and was much faster.