Generalizing the Legendre Symbol: Jacobi Symbol
Extra activity

In this activity, we will learn of a generalization of the Legendre symbol, called the *Jacobi symbol*, which can help in calculating the Legendre symbol. However, before we talk about the Jacobi symbol, let us figure out $\left(\frac{3}{p}\right)$ which was the last question in the last week's activity.

1 a. Using QR express $\left(\frac{3}{p}\right)$ in terms of $\left(\frac{p}{3}\right)$.

b. The value of the term $(-1)^*$ depends on the value of p modulo _____. So we consider two cases based on these moduli.

Case 1: When p is _____ modulo _____.

In this case, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$. But the value of $\left(\frac{p}{3}\right)$ depends on the value of p modulo 3. So we have two subcases, when $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$. In each subcase, determine the value of $\left(\frac{3}{p}\right)$.

Case 2: When p is _____ modulo _____.

Again, consider two subcases as in the previous case, and determine the value of $\left(\frac{3}{p}\right)$ in each subcase.

c. From your results above, there are four cases of p to consider in determining the value of $\left(\frac{3}{p}\right)$. All these cases are modulo 12. Using Chinese Remainder Theorem (or trial-error) determine what each of the four cases correspond to modulo 12.

Your work from the previous problem justifies the following proposition:

Proposition 1: Let $p \neq 2, 3$ be a prime. Then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \quad \pmod{12}, \\ -1 & \text{if } p \equiv \quad \pmod{12}. \end{cases}$$

Jacobi Symbol

Let a be any integer and n a positive odd integer with prime factorization $n = p_1 p_2 \cdots p_t$, where the p_i's are not necessarily distinct. Then the *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined as

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_t}\right)$$

where the right hand side terms are all Legendre symbols.

1. Find the value of $\left(\frac{2}{15}\right)$. Does 2 have a square root modulo 15?

Although the Legendre symbol $\left(\frac{a}{p}\right)$, by definition, gave us information about whether there was a square root of a modulo p, the Jacobi symbol does not give us a conclusive answer. If a is a square modulo n, then $\left(\frac{a}{n}\right) = 1$. This is because _____ _____ . But as you saw above, $\left(\frac{a}{n}\right) = 1$ does not imply that a is a square modulo n.

Properties of the Jacobi symbol: Let m, n be odd positive integers and a, b any integers. Suppose $m = q_1 q_2 \cdots q_r$ be a prime factorization of m, and $n = p_1 p_2 \cdots p_t$ be a prime factorization of n.

i. $\left(\frac{a}{n}\right) = 0$ if and only if _____.

ii. $\left(\frac{1}{n}\right) = 1$ because

iii. $\left(\frac{a^2}{n}\right) = 1$ because

iv. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$ because

v. $\left(\frac{-1}{n}\right) = 1$ if and only if $n \equiv 1 \pmod 4$. This follows because $\left(\frac{-1}{p}\right) = 1$ if $p \equiv \quad \pmod 4$ and $\left(\frac{-1}{p}\right) = -1$ if $p \equiv \quad \pmod 4$. To get a result of 1 for the Jacobi symbol, there must be an even number of p_i's such that $p_i \equiv \quad \pmod 4$. But then $n \equiv p_1 p_2 \cdots p_t \equiv \quad \pmod 4$ because $3 \cdot 3 \equiv \quad \pmod 4$.

Cont'd →

vi. $\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)$ because

vii. $\left(\frac{2}{n}\right) = 1$ if and only if $n \equiv \pm 1 \pmod 8$.

Similar to the QR for Legendre symbols, there is a QR relation for the Jacobi symbols.

Theorem 1: (Quadratic Reciprocity for Jacobi symbols) Let a and b be positive odd integers. Then

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/4}.$$

proof: Let us consider a special case of $a = p_1p_2$ and $b = q_1q_2q_3$ where p_i's and q_j's are primes. Then using the definition of the Jacobi symbol and the multiplicativity of the Legendre symbol, we find that

$$\left(\frac{a}{b}\right) = \qquad .$$

Now, using the QR for Legendre symbols, we find that

$$\left(\frac{a}{b}\right) =$$

Rearranging, we see that the $\left(\frac{q_j}{p_i}\right)$'s form $\left(\frac{b}{a}\right)$. To show that the product of the rest of the terms is $(-1)^{(a-1)(b-1)/2}$, we will use the following lemma.

Lemma: Let n be a positive odd integer with prime factorization $n = p_1p_2\cdots p_t$. Then

$$\frac{p_1-1}{2} + \frac{p_2-2}{2} + \cdots + \frac{p_t-1}{2} \equiv \frac{n-1}{2} \pmod 2.$$

Therefore,

$$(-1)^{(p_1-1)/2}(-1)^{(p_2-1)/2}\cdots(-1)^{(p_t-1)/2} = (-1)^{(n-1)/2}.$$

If we can prove this lemma, our proof of the QR for Jacobi symbols will be completed because

$$\begin{aligned}
\left(\frac{a}{b}\right) &= \left(\frac{b}{a}\right)\left((-1)^{(q_1-1)/2}(-1)^{(q_2-1)/2}(-1)^{(q_3-1)/2}\right)^{(p_1-1)/2}\left((-1)^{(q_1-1)/2}(-1)^{(q_2-1)/2}(-1)^{(q_3-1)/2}\right)^{(p_2-1)/2} \\
&= \left(\frac{b}{a}\right)\left((-1)^{(b-1)/2}\right)^{(p_1-1)/2}\left((-1)^{(b-1)/2}\right)^{(p_2-1)/2} \\
&= \left(\frac{b}{a}\right)\left((-1)^{(p_1-1)/2}(-1)^{(p_2-1)/2}\right)^{(b-1)/2} \\
&= \left(\frac{b}{a}\right)\left((-1)^{(a-1)/2}\right)^{(b-1)/2} = \left(\frac{b}{a}\right)(-1)^{(a-1)(b-1)/4}
\end{aligned}$$

This is the statement of the QR for Jacobi symbols.

Now let us prove the lemma.

proof: (Lemma) Reordering the primes p_i, if necessary, assume that the first r of the primes are congruent to 3 modulo 4 and the rest are congruent to 1 modulo 4. Using the same logic as in the proof of property v of the Jacobi symbols, $n \equiv 1 \pmod 4$ if and only if r is even. Hence $(n-1)/2 \equiv 0 \pmod 2$ if and only if r is even.

For each of the first r primes, $(p_i-1)/2 \equiv 1 \pmod 4$, while for the others, $(p_i-1)/2 \equiv 0 \pmod 4$. Therefore,

$$\frac{p_1-1}{2} + \frac{p_2-1}{2} + \cdots + \frac{p_t-1}{2} \equiv r \pmod 4 .$$

So the sum is congruent to 0 modulo 2 if and only if r is even, which happens if and only if $(n-1)/2$ is congruent to 0 modulo 2.

The second half of the Lemma follows from the exponent properties.

□

Note: With the QR for Jacobi symbols, we do not have to worry about factoring either the a or b. This is especially useful when a and b are large integers and factoring them would be a lot of work.

2. Use the QR for Jacobi symbols and the properties of the Jacobi symbols to determine the following. (Note: You can use QR only for odd positive integers.)

a. $\left(\frac{55}{77}\right)$

b. $\left(\frac{55}{79}\right)$

c. (If time) $\left(\frac{481}{3977}\right)$