SECTION 7.5 ➡️ **Quadratic Residues of Composite Moduli**

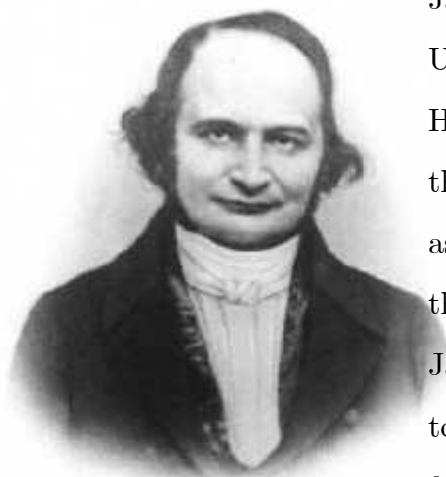By the end of this section you will be able to

- distinguish between Jacobi and Legendre symbols
- determine which integers are quadratic residues of composite moduli

7.5.1 Testing Integers of Composite Moduli

The Law of Quadratic Reciprocity – LQR and its corollary are powerful methods to evaluate the Legendre symbol $\left(a\,/\,p\right)$ where p is an odd prime. Say we wanted to find $\left(a\,/\,n\right)$ where n is a composite integer. This $\left(a\,/\,n\right)$ *cannot* be the Legendre symbol because we need $n = p$ where p is an odd prime for the Legendre symbol.

We can use LQR and its corollary but we would have to factorize a and n into its prime decomposition. *For small integers a and n it is smooth enough but what if these integers are not small?*

We extend the Legendre symbol to cover integers a and n where n is any odd integer greater than 1 and both integers a and n are *relatively prime*. This generalized Legendre symbol is called the Jacobi symbol named after Carl Jacobi pronounced Yah Koh Bee.

Jacobi was of Jewish origin, actually in order to teach at the University of Berlin he converted to Christianity in 1825. He was academically a very bright school child and went to the University of Berlin in 1821. He excelled in mathematics as well as in other subjects at the university. He moved to the University of Königsberg in 1826.

Jacobi made serious contributions to number theory on topics such as quadratic and cubic residues and elliptic functions. He also produced research in partial differential equations and determinants.

Figure 16 Jacobi 1804 - 51

He became professor in 1832 but in 1843 he left Könsigberg and went to Italy for health reasons. However, he was back in Berlin by 1844 and delivered lectures at the University of Berlin. He died of small box in 1851.

Definition (7.21).

Let a and n be integers where n is an odd integer greater than 1 and $\gcd(a, \ n) = 1$.

Also let $n = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_m^{k_m}$ be the prime decomposition of n. The Jacobi symbol,

$\left(\dfrac{a}{n}\right)$ or $\left(a/n\right)$, is defined by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \times \left(\frac{a}{p_2}\right)^{k_2} \times \cdots \times \left(\frac{a}{p_m}\right)^{k_m} \quad \text{where} \ \left(\frac{a}{p_j}\right) \text{ is the Legendre symbol.}$$

Example 7.21

Compute the Jacobi symbol $\left(8/15\right)$.

Solution

As 15 is composite so $\left(8/15\right)$ is a Jacobi symbol. The prime factorization of 15 is 3×5.

Applying the above defined Jacobi symbol we have

$$\left(\frac{8}{15}\right) = \left(\frac{8}{3 \times 5}\right) = \left(\frac{8}{3}\right) \times \left(\frac{8}{5}\right) \qquad \left[\begin{array}{l} \text{These are now Legendre symbols on the} \\ \text{right-hand side because 3 and 5 are prime.}\end{array}\right]$$

$$= \left(\frac{2}{3}\right) \times \left(\frac{3}{5}\right) \qquad \left[\text{Because } 8 \equiv 2 \ (\text{mod } 3) \ \text{ and } \ 8 \equiv 3 \ (\text{mod } 5)\right]$$

$$= \left(\frac{2}{3}\right) \times \underbrace{\left(\frac{5}{3}\right)}_{\text{by Corollary (7.17)}} \quad = \left(\frac{2}{3}\right) \times \left(\frac{2}{3}\right) \qquad \left[\text{Because } 5 \equiv 2 \ (\text{mod } 3)\right]$$

Using the test for residue 2 from previous sections:

(7.15)
$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } \ p \equiv \pm 1 \ (\text{mod } 8) \\ -1 & \text{if } \ p \equiv \pm 3 \ (\text{mod } 8) \end{cases}$$

With $p \equiv 3 \ (\text{mod } 8)$ we have

$$\left(\frac{8}{15}\right) = \left(\frac{2}{3}\right) \times \left(\frac{2}{3}\right) = \left(-1\right) \times \left(-1\right) = 1$$

There is one *hiccup* in using the Jacobi symbol, that is if $\left(\dfrac{a}{n}\right) = 1$ then this does *not*

imply that a is a quadratic residue of n. Consider the above example, we have

$$\left(\frac{8}{15}\right) = \left(\frac{8}{3}\right) \times \left(\frac{8}{5}\right) = (-1) \times (-1) = 1$$

The right-hand side $(-1) \times (-1)$ tells us that there are *no* solutions to the quadratic

$$x^2 \equiv 8 \pmod{3} \text{ and } x^2 \equiv 8 \pmod{5}$$

Applying the Chinese Remainder Theorem (3.22) of Chapter 3 to this implies that there

are *no* solutions to the quadratic congruence $x^2 \equiv 8 \left(\bmod \left[3 \times 5\right]\right) \equiv 8 \pmod{15}$.

In general if $\left(a \ / \ n\right) = 1$ then a is a quadratic residue of n $\Leftrightarrow$ *all* Legendre symbols in

the calculation $\left(a \ / \ p\right) = 1$ where p is an odd prime in the decomposition of n.

If the quadratic congruence $x^2 \equiv a \pmod{n}$ has a solution, then the Jacobi symbol

$\left(a \ / \ n\right) = 1$. However, if $\left(a \ / \ n\right) = 1$ we *cannot* conclude that $x^2 \equiv a \pmod{n}$ has a

solution. In the above example we had $\left(8 \ / \ 15\right) = 1$ but there are *no* solutions to

$x^2 \equiv 8 \pmod{15}$.

In addition, if the Jacobi symbol $\left(a \ / \ n\right) = -1$ then the quadratic congruence

$x^2 \equiv a \pmod{n}$ has *no* solutions.

7.5.2 Properties of the Jacobi Symbol

Proposition (7.22).

Let n be an odd integer greater than 1. Let a and b be integers relatively prime to n.

We have

(a)   If $a \equiv b \pmod{n}$ then the Jacobi symbol $\left(\dfrac{a}{n}\right) = \left(\dfrac{b}{n}\right)$.

(b)   The Jacobi symbol $\left(\dfrac{a \times b}{n}\right) = \left(\dfrac{a}{n}\right) \times \left(\dfrac{b}{n}\right)$ - multiplicative property.

(c)   The Jacobi symbol $\left(\dfrac{a^2}{n}\right) = 1$.

How do we prove these?

Since we have results about Legendre symbols so we use these but first we need to write

n in its prime decomposition:

$$n = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_m^{k_m}$$

Proof of (a):

By question 24(e) of Exercises 3.1 we have if $a \equiv b \pmod{n}$ then $a \equiv b \pmod{p_j}$ for

$j = 1, 2, \cdots, m$. As we have $a \equiv b \pmod{p_j}$ so we can use Proposition (7.9) part (a):

$$a \equiv b \pmod{p} \ \text{ implies } \ \left(a/p\right) = \left(b/p\right)$$

Applying the Jacobi symbol as defined in (7.21) we have

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_m^{k_m}}\right) = \left(\frac{a}{p_1}\right)^{k_1} \times \left(\frac{a}{p_2}\right)^{k_2} \times \cdots \times \left(\frac{a}{p_m}\right)^{k_m} \qquad \left[\text{By (7.21)}\right]$$

$$= \left(\frac{b}{p_1}\right)^{k_1} \times \left(\frac{b}{p_2}\right)^{k_2} \times \cdots \times \left(\frac{b}{p_m}\right)^{k_m} \qquad \left[\text{By (7.9) part (a)}\right]$$

$$= \left(\frac{b}{p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_m^{k_m}}\right) \qquad \left[\text{By (7.21)}\right]$$

$$= \left(\frac{b}{n}\right) \qquad \left[\text{Because } n = p_1^{k_1} \times \cdots \times p_m^{k_m}\right]$$

Proof of (b):

Since we need to prove $\left(\dfrac{a \times b}{n}\right) = \left(\dfrac{a}{n}\right) \times \left(\dfrac{b}{n}\right)$ so we use Proposition (7.9) part (c):

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

By using this property, we have $\left(\dfrac{a \times b}{p_j}\right) = \left(\dfrac{a}{p_j}\right) \times \left(\dfrac{b}{p_j}\right)$ for $j = 1, 2, \cdots, m$.

Again using the prime factorization of n so that we can apply the above property:

$$\left(\frac{a \times b}{n}\right) = \left(\frac{a \times b}{p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_m^{k_m}}\right) = \left(\frac{a \times b}{p_1}\right)^{k_1} \times \left(\frac{a \times b}{p_2}\right)^{k_2} \times \cdots \times \left(\frac{a \times b}{p_m}\right)^{k_m} \quad \left[\begin{array}{l}\text{By} \\ \text{definition (7.21)}\end{array}\right]$$

$$= \left[\left(\frac{a}{p_1}\right) \times \left(\frac{b}{p_1}\right)\right]^{k_1} \times \cdots \times \left[\left(\frac{a}{p_m}\right) \times \left(\frac{b}{p_m}\right)\right]^{k_m} \quad \left[\text{By (7.9) part (c)}\right]$$

$$\underset{\text{rearranging}}{=} \left[\left(\frac{a}{p_1}\right)^{k_1} \times \cdots \times \left(\frac{a}{p_m}\right)^{k_m}\right] \times \left[\left(\frac{b}{p_1}\right)^{k_1} \times \cdots \times \left(\frac{b}{p_m}\right)^{k_m}\right]$$

$$= \left(\frac{a}{n}\right) \times \left(\frac{b}{n}\right) \quad \left[\begin{array}{l}\text{By} \\ \text{definition (7.21)}\end{array}\right]$$

We have $\left(\dfrac{a \times b}{n}\right) = \left(\dfrac{a}{n}\right) \times \left(\dfrac{b}{n}\right)$ which is our required result.

Proof of (c):

Let $x \equiv \pm a \left(\mathrm{mod}\ n\right)$ then $x^2 \equiv a^2 \left(\mathrm{mod}\ n\right)$ so this quadratic congruence has a solution which implies that $\left(a^2\ /\ n\right) = 1$. This completes our proof.

Example 7.22

Compute the following Jacobi symbols:

(a) $\left(\dfrac{49}{15}\right)$ 　　　　　　　(b) $\left(\dfrac{59}{21}\right)$ 　　　　　　　(c) $\left(\dfrac{12}{35}\right)$

Solution

(a) The prime decomposition of $49 = 7^2$ so we have

$$\left(\frac{49}{15}\right) = \left(\frac{7^2}{15}\right) = 1 \qquad \left[\text{By above Proposition (7.22) part (c) } \left(\frac{a^2}{n}\right) = 1\right]$$

(b) Firstly $59 \equiv 17 \left(\mathrm{mod}\ 21\right)$ so by Proposition (7.22) part (a):

$$a \equiv b \left(\mathrm{mod}\ n\right) \text{ implies } \left(a\ /\ n\right) = \left(b\ /\ n\right)$$

We have $\left(\dfrac{59}{21}\right) = \left(\dfrac{17}{21}\right)$. The prime decomposition of $21 = 3 \times 7$. Therefore

$$\left(\frac{17}{21}\right) = \left(\frac{17}{3 \times 7}\right) \underset{\text{By (7.21)}}{=} \left(\frac{17}{3}\right) \times \left(\frac{17}{7}\right) = \left(\frac{2}{3}\right) \times \left(\frac{3}{7}\right) \qquad \left[\begin{array}{l}\text{Because } 17 \equiv 2 \left(\mathrm{mod}\ 3\right) \\ \text{and } 17 \equiv 3 \left(\mathrm{mod}\ 7\right)\end{array}\right]$$

$$= \left(\frac{2}{3}\right) \times \left[-\left(\frac{7}{3}\right)\right] \qquad \left[\begin{array}{l}\text{By Corollary (7.17)} \\ \text{because } 7 \equiv 3 \left(\mathrm{mod}\ 4\right)\end{array}\right]$$

$$= \left(\frac{2}{3}\right) \times \left[-\left(\frac{1}{3}\right)\right] \qquad \left[\text{Because } 7 \equiv 1 \left(\mathrm{mod}\ 3\right)\right]$$

$$= \left(\frac{2}{3}\right) \times \left[-1\right] = -\left(\frac{2}{3}\right) \qquad \left[\text{Because } \left(\frac{1}{3}\right) = 1 \text{ as 1 is a QR}\right]$$

Now we use the test for residue 2 modulo p:

(7.15) 　　　　　　　　$\left(\dfrac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \left(\mathrm{mod}\ 8\right) \\ -1 & \text{if } p \equiv \pm 3 \left(\mathrm{mod}\ 8\right) \end{cases}$

We apply this to the above calculation with prime $p \equiv 3 \left(\text{mod } 8\right)$:

$$\left(\frac{17}{21}\right) = -\left(\frac{2}{3}\right) = -\left(-1\right) = 1$$

Hence $\left(\frac{59}{21}\right) = \left(\frac{17}{21}\right) = 1$. Although $\left(\frac{59}{21}\right) = 1$ but $x^2 \equiv 59 \left(\text{mod } 21\right)$ has *no* solutions

because from above we have $\left(\frac{59}{21}\right) = \left(\frac{17}{21}\right) = \left(\frac{17}{3}\right) \times \left(\frac{17}{7}\right) = \left(-1\right) \times \left[-1\right] = 1$.

(c) We need to find the Jacobi symbol $\left(\frac{12}{35}\right)$. The prime decomposition of $12 = 2^2 \times 3$

and 2 and 3 are relatively prime so by Proposition (7.22) part (b):

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

We have

$$\left(\frac{12}{35}\right) = \underbrace{\left(\frac{2^2}{35}\right)}_{=1 \text{ by (7.22) part (c)}} \times \left(\frac{3}{35}\right) = 1 \times \left(\frac{3}{35}\right) = \left(\frac{3}{35}\right) \quad (*)$$

The prime decomposition $35 = 5 \times 7$ therefore

$$\left(\frac{3}{35}\right) = \left(\frac{3}{5 \times 7}\right) = \left(\frac{3}{5}\right) \times \left(\frac{3}{7}\right) \qquad \left[\text{By definition (7.21) of the Jacobi symbol}\right]$$

$$= \left(\frac{5}{3}\right) \times \left[-\left(\frac{7}{3}\right)\right] \qquad \left[\begin{array}{l}\text{By (7.17) because we are now working} \\ \text{with Legendre symbols}\end{array}\right]$$

$$= \left(\frac{2}{3}\right) \times \left[-\left(\frac{1}{3}\right)\right] \qquad \left[\text{Because } 5 \equiv 2 \left(\text{mod } 3\right) \text{ and } 7 \equiv 1 \left(\text{mod } 3\right)\right]$$

$$= \left(-1\right) \times \left(-1\right) = 1 \qquad \left[\text{By the calculation of part (b)}\right]$$

Putting this result $\left(\frac{3}{35}\right) = 1$ into (*) gives $\left(\frac{12}{35}\right) = \left(\frac{3}{35}\right) = 1$.

In this case we have $\left(12 \,/\, 35\right) = 1$ but the quadratic congruence $x^2 \equiv 12 \left(\text{mod } 35\right)$ does

not have solutions because of the presence of -1 in the above calculation.

7.5.3 Testing Residues -1 and 2

For the Legendre symbols we stated properties for testing the residues -1 and 2. In the

same manner we find properties which give us easy ways of testing $\left(\dfrac{-1}{n}\right)$ and $\left(\dfrac{2}{n}\right)$

where $n > 1$ is an odd *composite* integer. In sight of this we carry out the following numerical example.

Example 7.23

Compute the Jacobi symbol $\left(\dfrac{-1}{105}\right)$. Also determine $(-1)^{\frac{1}{2}(n-1)}$ with $n = 105$.

Solution

The prime decomposition of $105 = 3 \times 5 \times 7$. Using definition of Jacobi symbol (7.21):

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \times \left(\frac{a}{p_2}\right)^{k_2} \times \cdots \times \left(\frac{a}{p_m}\right)^{k_m} \quad \text{where } n = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_m^{k_m}$$

With $105 = 3 \times 5 \times 7$ we have

$$\left(\frac{-1}{105}\right) = \left(\frac{-1}{3 \times 5 \times 7}\right) = \left(\frac{-1}{3}\right) \times \left(\frac{-1}{5}\right) \times \left(\frac{-1}{7}\right) \qquad (\ddagger)$$

For testing the residue -1 we use Proposition (7.11):

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

By applying this result with $p \equiv 3$, $p \equiv 5 \equiv 1$ and $p \equiv 7 \equiv 3 \;(\text{mod } 4)$ it follows that

$$\left(\frac{-1}{3}\right) = -1, \; \left(\frac{-1}{5}\right) = 1 \text{ and } \left(\frac{-1}{7}\right) = -1 \text{ respectively.}$$

Substituting these into $(\ddagger)$ gives

$$\left(\frac{-1}{105}\right) = \left(\frac{-1}{3}\right) \times \left(\frac{-1}{5}\right) \times \left(\frac{-1}{7}\right) = (-1) \times 1 \times (-1) = 1$$

Evaluating $(-1)^{\frac{1}{2}(n-1)}$ with $n = 105$ yields

$$(-1)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(105-1)} = (-1)^{52} = 1$$

Note that $\left(\dfrac{-1}{105}\right) = (-1)^{\frac{1}{2}(105-1)} = 1$.

This Jacobi symbol $\left(\dfrac{-1}{105}\right) = (-1)^{\frac{1}{2}(105-1)}$ is *not* just true for $n = 105$ but is generally true;

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{1}{2}(n-1)} \text{ for any odd integer } n \text{ greater than 1.}$$

Evidently you can see that it is much easier to use the right-hand expression $(-1)^{\frac{1}{2}(n-1)}$ to evaluate the Jacobi symbol $(-1/n)$.

Similarly, we have a result for testing the Jacobi symbol $(2/n)$.

To prove these general results we need a lemma.

Lemma (7.23).

Let n be an odd integer greater than 1 and its prime decomposition $n = \prod_{j=1}^{m} p_j^{k_j}$. Then

(a) $\displaystyle\sum_{j=1}^{m} k_j \frac{(p_j - 1)}{2} \equiv \frac{n-1}{2} \pmod 2$

(b) $\displaystyle\sum_{j=1}^{m} k_j \frac{(p_j^2 - 1)}{8} \equiv \frac{n^2 - 1}{8} \pmod 2$

Proof.

See question 11 of Exercise 7.5.

Proposition (7.24).

Let n be an odd integer greater than 1 then

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

Proof of (a). Let the prime decomposition of $n = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_m^{k_m}$. Then

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)^{k_1} \times \left(\frac{-1}{p_2}\right)^{k_2} \times \left(\frac{-1}{p_3}\right)^{k_3} \times \cdots \times \left(\frac{-1}{p_m}\right)^{k_m} \qquad \left[\text{By the Jacobi symbol definition (7.21)}\right]$$

$$= \left[(-1)^{\frac{p_1-1}{2}}\right]^{k_1} \times \left[(-1)^{\frac{p_2-1}{2}}\right]^{k_2} \times \cdots \times \left[(-1)^{\frac{p_m-1}{2}}\right]^{k_m} \qquad \left[\text{By q8 of Exercise 7(b)} \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}\right]$$

$$= (-1)^{k_1\left(\frac{p_1-1}{2}\right)} \times (-1)^{k_2\left(\frac{p_2-1}{2}\right)} \times \cdots \times (-1)^{k_m\left(\frac{p_m-1}{2}\right)} \qquad \left[\text{By rules of indices} \quad (a^x)^y = a^{xy}\right]$$

$$= (-1)^{k_1\left(\frac{p_1-1}{2}\right) + k_2\left(\frac{p_2-1}{2}\right) + \cdots + k_m\left(\frac{p_m-1}{2}\right)} \qquad \left[\text{By rules of indices} \quad a^x a^y = a^{x+y} \text{ with } a = (-1)\right]$$

$$= (-1)^{\sum_{j=1}^{m} k_j\left(\frac{p_j-1}{2}\right)} = (-1)^{\frac{1}{2}(n-1)} \qquad \left[\text{By (7.23) (a)} \sum_{j=1}^{m} k_j \frac{(p_j - 1)}{2} \equiv \frac{n-1}{2} \pmod 2\right]$$

This completes our proof.

Proof of (b): See question 12 of Exercise 7.5.

It is much easier to use this Proposition (7.24) to evaluate the Jacobi symbol $\left(-1/n\right)$

and $\left(2/n\right)$. For example

$$\left(\frac{-1}{1001}\right) = \left(-1\right)^{\frac{1}{2}(1001-1)} = \left(-1\right)^{500} = 1$$

$$\left(\frac{2}{99}\right) = \left(-1\right)^{\frac{1}{8}\left(99^2-1\right)} = \left(-1\right)^{1225} = -1$$

Now we extend the Law of Quadratic Residues, LQR, to any odd integers greater than 1. In LQR we were restricted to primes p and q.

7.5.4 General Law of Quadratic Reciprocity

We have analogous result for odd integers greater than 1:

The General Law of Quadratic Reciprocity GLQR (7.25).

Let m and n be odd integers greater than 1 and be relatively prime then

$$\left(\frac{n}{m}\right) \times \left(\frac{m}{n}\right) = \left(-1\right)^{\left(\frac{n-1}{2}\right)\times\left(\frac{m-1}{2}\right)}$$

How do we prove this result?

We use our LQR result.

Proof. See question 13 of Exercises 7.5.

Corollary (7.26).

Let m and n be odd integers greater than 1 and be relatively prime. Then

$$\left(\frac{m}{n}\right) = \begin{cases} \left(n / m\right) & \text{if } m \equiv 1 \pmod 4 \text{ or } n \equiv 1 \pmod 4 \\ -\left(n / m\right) & \text{if } m \equiv n \equiv 3 \pmod 4 \end{cases}$$

Proof. See question 5 of Exercise 7.5.

Next, we apply this Corollary to a numerical example.

Example 7.24

Compute the Jacobi symbol $\left(\dfrac{715}{291}\right)$. (Note 291 is composite.)

Solution

First we use Proposition (7.22) part (a) to reduce our arithmetic calculation:

If $a \equiv b \pmod{n}$ then $\left(\dfrac{a}{n}\right) = \left(\dfrac{b}{n}\right)$.

Since $715 \equiv 133 \pmod{291}$ so by using this proposition we have

$$\left(\frac{715}{291}\right) = \left(\frac{133}{291}\right)$$

As $133 \equiv 1 \pmod{4}$ so by Corollary (7.26):

$$\left(\frac{m}{n}\right) = \begin{cases} (n \,/\, m) & \text{if } m \equiv 1 \pmod{4} \text{ or } n \equiv 1 \pmod{4} \\ -(n \,/\, m) & \text{if } m \equiv n \equiv 3 \pmod{4} \end{cases}$$

We have $\left(\dfrac{133}{291}\right) = \left(\dfrac{291}{133}\right) = \left(\dfrac{25}{133}\right)$ because $291 \equiv 25 \pmod{133}$. Since $25 = 5^2$ so

$$\left(\frac{25}{133}\right) = 1 \quad \left[\text{Because by (7.22) (c) } \left(\frac{a^2}{n}\right) = 1\right]$$

Hence $\left(\dfrac{715}{291}\right) = 1$. In this case we have solutions to $x^2 \equiv 715 \pmod{291}$.

Summary

In this section we extend the LQR to cover composite odd integers m and n.

Corollary (7.26) is useful in evaluating Jacobi symbols:

(7.26) $\left(\dfrac{m}{n}\right) = \begin{cases} (n \,/\, m) & \text{if } m \equiv 1 \pmod{4} \text{ or } n \equiv 1 \pmod{4} \\ -(n \,/\, m) & \text{if } m \equiv n \equiv 3 \pmod{4} \end{cases}$