4.2. **The Jacobi symbol.** The Legendre symbol $(\frac{a}{p})$ indicates whether an integer $a$ not divisible by an odd prime $p$ is a quadratic residue modulo $p$. We have seen how to use quadratic reciprocity to compute it. However this requires to factor $a$ into primes, which is in general a hard problem when $a$ is large. To make the computation easier, we introduce the following generalisation of the Legendre symbol:

**Definition 4.9.** Let $a$ be any integer and $b$ be a positive odd integer. Let $b = p_1 p_2 \cdots p_m$ be its prime factorisation, where $p_1, p_2, \cdots, p_m$ are not necessarily distinct primes. The symbol $\left(\frac{a}{b}\right)$ defined by

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_m}\right)$$

is called the *Jacobi symbol*.

The notation for the Jacobi symbol is identical to that for the Legendre symbol. Indeed, when $b$ is an odd prime, the Jacobi symbol $(\frac{a}{b})$ is precisely the corresponding Legendre symbol by definition. Moreover, the Jacobi symbol has properties that are remarkably similar to the Legendre symbol. However, we should also be aware of their difference. We immediately point out some important differences between the two symbols before we show their similarities.

*Remark* 4.10. We illustrate the following differences between the two symbols by examples.

(1) For $(\frac{a}{b})$, as a Legendre symbol we require that $b$ is a positive odd prime, while as a Jacobi symbol we only require that $b$ is a positive odd integer. So $(\frac{6}{11})$ can be interpreted either as a Legendre symbol or a Jacobi symbol, while $(\frac{14}{45})$ must be a Jacobi symbol.

(2) The Jacobi symbol is in general not an indicator for quadratic residues. That is, $(\frac{a}{b})$ may equal 1 without $a$ being a quadratic residue modulo $b$. For example, $(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1)(-1) = 1$, but 2 is not a quadratic residue modulo 15, because if $x^2 \equiv 2 \pmod{15}$ has a solution, then the same integer value of $x$ is a solution to $x^2 \equiv 2 \pmod 3$, which is impossible. It is true, however, that if $(\frac{a}{b}) = -1$, then $a$ is a quadratic non-residue modulo $b$; see Exercise 4.3 (1).

(3) In comparison to Proposition 4.4 (1), $(\frac{a}{b})$ and $a^{\frac{b-1}{2}}$ are in general not congruent modulo $b$ in case of the Jacobi symbol. For example, $(\frac{2}{15}) \not\equiv 2^{\frac{15-1}{2}} \pmod{15}$ because $(\frac{2}{15}) = 1$ while $2^7 \equiv 8 \pmod{15}$.

Now we turn to the properties of the Jacobi symbol. Apart from what was mentioned above, most of the properties of the Jacobi symbol are extremely similar to those of the Legendre symbol. As a result, the computation of Jacobi symbols are also very similar to that of Legendre symbols, even easier.

The basic idea behind all their proofs is to use the definition to rewrite everything in terms of the Legendre symbol and apply the corresponding properties of the Legendre symbol. We list all the properties and prove only the first one as a sample of the proofs. One more proof will be left as an exercise for you to try yourself; see Exercise 4.3 (2).

**Proposition 4.11.** *Let $b$ be a positive odd integer.*

(1) *If* $a_1 \equiv a_2 \pmod{b}$, *then* $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$.

(2) *If* $\mathrm{hcf}(a, b) = 1$, *then* $\left(\frac{a^2}{b}\right) = 1$.

*Proof.* Both statements are consequences of Definition 4.9 and Proposition 4.3. We assume $b = p_1 p_2 \cdots p_m$ is the prime factorisation of $b$, where $p_1, p_2, \cdots, p_m$ are not necessarily distinct primes. For (1), by definition and Proposition 4.3 (1) we have

$$\left(\frac{a_1}{b}\right) = \left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\cdots\left(\frac{a_1}{p_m}\right) = \left(\frac{a_2}{p_1}\right)\left(\frac{a_2}{p_2}\right)\cdots\left(\frac{a_2}{p_m}\right) = \left(\frac{a_2}{b}\right).$$

For (2), since $p_i \nmid a$ for each $i$, by definition and Proposition 4.3 (2) we have

$$\left(\frac{a^2}{b}\right) = \left(\frac{a^2}{p_1}\right)\left(\frac{a^2}{p_2}\right)\cdots\left(\frac{a^2}{p_m}\right) = 1.$$

□

**Proposition 4.12.** *Let $b, b_1, b_2$ be positive odd integers.*

(1) $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$.

(2) $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$.

**Proposition 4.13.** *Let $b$ be a positive odd integer.*

(1) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} = \begin{cases} 1 & \text{if } b \equiv 1 \pmod{4} \\ -1 & \text{if } b \equiv -1 \pmod{4}. \end{cases}$

(2) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} = \begin{cases} 1 & \text{if } b \equiv \pm 1 \pmod{8} \\ -1 & \text{if } b \equiv \pm 3 \pmod{8}. \end{cases}$

**Proposition 4.14** (Quadratic Reciprocity for the Jacobi symbol)**.** *Let $a, b$ be coprime positive odd integers. Then*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}.$$

The Jacobi symbol is very useful. We are mainly interested in using it to calculate Legendre symbols. Roughly speaking, aside from pulling out factors of $-1$ and 2 as they arise, one can proceed with quadratic reciprocity without worrying about whether or not the numerator is a prime. We show the procedure in the following example.

**Example 4.15.** Given 1151 is a prime, we compare the two calculations for the Legendre symbol $(\frac{1003}{1151})$.

Without using the Jacobi symbol, we need to factor the numerator $1003 = 17 \times 59$ (it takes some effort to get this!). Hence $(\frac{1003}{1151}) = (\frac{17}{1151})(\frac{59}{1151})$. Since 17 is congruent to 1 modulo 4, we have $(\frac{17}{1151}) = (\frac{1151}{17}) = (\frac{12}{17}) = (\frac{4}{17})(\frac{3}{17}) = (\frac{3}{17})$. By the same reason $(\frac{3}{17}) = (\frac{17}{3}) = (\frac{2}{3}) = -1$. On the other hand since both 59 and 1151 are congruent to $-1$ modulo 4, we have $(\frac{59}{1151}) = -(\frac{1151}{59}) = -(\frac{30}{59}) = -(\frac{2}{59})(\frac{3}{59})(\frac{5}{59})$. Since $59 \equiv 3 \pmod 8$ we get $(\frac{2}{59}) = -1$. Since $3 \equiv 59 \equiv -1 \pmod 4$ we get $(\frac{3}{59}) = -(\frac{59}{3}) = -(\frac{2}{3}) = 1$. Since $5 \equiv 1 \pmod 4$ we get $(\frac{5}{59}) = (\frac{59}{5}) = (\frac{4}{5}) = 1$. All this together shows $(\frac{59}{1151}) = -1$.

Using the Jacobi symbol, we can avoid the prime factorisation, so the calculation is much simpler. Since 1003 and 1151 are both congruent to $-1$ modulo 4, the quadratic reciprocity gives $(\frac{1003}{1151}) = -(\frac{1151}{1003}) = -(\frac{148}{1003}) = -(\frac{4}{1003})(\frac{37}{1003}) = -(\frac{37}{1003})$. Since $37 \equiv 1 \pmod 4$, we have $(\frac{37}{1003}) = (\frac{1003}{37}) = (\frac{4}{37}) = 1$. Hence $(\frac{1003}{1151}) = -1$. Works like a charm!

Now we switch gears and discuss a more significant application of the Legendre and Jacobi symbols. From Proposition 4.5 we noticed that $-1$ is a quadratic residue for primes of the form $4k+1$ and that 2 is a quadratic residue for primes of the form $8k \pm 1$. If $a$ is an arbitrary integer, for what odd primes $p$ is $a$ a quadratic residue modulo $p$? We illustrate this type of questions using the following example.

**Example 4.16.** To find all odd primes $p$ for which 3 is a quadratic residue, we need to compute $(\frac{3}{p})$ for all $p \neq 3$. To apply quadratic reciprocity, we need to consider two cases.

If $p \equiv 1 \pmod 4$, then $(\frac{3}{p}) = (\frac{p}{3})$, which is 1 if $p \equiv 1 \pmod 3$, or $-1$ if $p \equiv 2 \pmod 3$. We can solve the system of the congruences modulo 3 and 4 to obtain: $(\frac{p}{3}) = 1$ if $p \equiv 1 \pmod{12}$, or $-1$ if $p \equiv 5 \pmod{12}$. (Please fill in the details of the computation.)

On the other hand, if $p \equiv 3 \pmod 4$, then $(\frac{3}{p}) = -(\frac{p}{3})$. Still, $(\frac{p}{3}) = 1$ if $p \equiv 1 \pmod 3$, or $-1$ if $p \equiv 2 \pmod 3$. We can solve the system of the congruences modulo 3 and 4 to obtain: $(\frac{p}{3}) = 1$ if $p \equiv 7 \pmod{12}$, or $-1$ if $p \equiv 11 \pmod{12}$. (Please fill in the details of the computation.)

| | $p \equiv 1 \pmod 4$ | $p \equiv 3 \pmod 4$ |
|---|---|---|
| $p \equiv 1 \pmod 3$ | $(\frac{3}{p}) = 1, p \equiv 1 \pmod{12}$ | $(\frac{3}{p}) = -1, p \equiv 7 \pmod{12}$ |
| $p \equiv 2 \pmod 3$ | $(\frac{3}{p}) = -1, p \equiv 5 \pmod{12}$ | $(\frac{3}{p}) = 1, p \equiv 11 \pmod{12}$ |

Summarising the above results, we get

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if} \quad p \equiv 1 \text{ or } 11 \pmod{12} \\ -1 & \text{if} \quad p \equiv 5 \text{ or } 7 \pmod{12}. \end{cases}$$

In other words, 3 is a quadratic residue for an odd prime $p$ iff $p \equiv \pm 1 \pmod{12}$.