# Primes - Handout 3

## Jacobi symbols (NON-EXAMINABLE)

Our aim is to sketch the proof of the following Lemma, in particular giving the construction of the group homomorphism $\chi$, described therein.

**Lemma 1.** *If $D \equiv 0, 1 \pmod 4$ is a non-zero integer (in particular, a discriminant). Then there is a unique group homomorphism*

$$\chi\colon (\mathbb{Z}/D\mathbb{Z})^* \to \{\,\pm 1\,\}$$

*such that $\chi([p]) = \left(\frac{D}{p}\right)$ for odd primes $p \nmid D$.*

## Jacobi symbol, definition and properties

We extend the Legendre symbol $\left(\dfrac{a}{p}\right)$, defined only for prime $p$, to a symbol

$$\left(\frac{M}{m}\right),$$

defined for any $m > 0$, odd, positive and coprime to $M$.

**Definition 2** (Jacobi symbol)**.** Let $M$ be an integer, and $m > 0$ be an odd, positive integer, coprime to $M$. Suppose $m = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorisation of $m$. Then we define

$$\left(\frac{M}{m}\right) \coloneqq \prod_{i=1}^{r} \left(\frac{M}{p_i}\right)^{e_i},$$

by extending the Legendre symbol multiplicatively to the lower argument.

[If $\gcd(M, m) = 1$, one can define

$$\left(\frac{M}{m}\right) = 0$$

to extend the Legendre symbol to all odd $m$.]

Some properties of this symbol are easy to see immediately

- If $M \equiv N \pmod m$, then $\left(\dfrac{M}{m}\right) = \left(\dfrac{N}{m}\right)$.
- $\left(\dfrac{MN}{m}\right) = \left(\dfrac{M}{m}\right)\left(\dfrac{N}{m}\right)$,
- $\left(\dfrac{M}{mn}\right) = \left(\dfrac{M}{m}\right)\left(\dfrac{M}{n}\right)$

**Proposition 3** (Quadratic reciprocity for Jacobi symbols)**.** *The Jacobi symbol* $\left(\frac{M}{m}\right)$ *satisfies the following quadratic reciprocity laws*

- $\left(\dfrac{M}{m}\right) = (-1)^{(M-1)(m1)/4}\left(\dfrac{m}{M}\right)$
- $\left(\dfrac{-1}{m}\right) = (-1)^{(m-1)/2}$
- $\left(\dfrac{2}{m}\right) = (-1)^{(m^2-1)/8}$

*Sketch.* These follow from quadratic reciprocity, and the supplementary laws for $\left(\frac{D}{p}\right)$. Make use of the following identities for $r, s$ odd

$$(rs-1)/2 \equiv (r-1)/2 + (s-1)/2 \pmod 2$$
$$((rs)^2-1)/8 \equiv (r^2-1)/8 + (s^2-1)/8 \pmod 2\,.$$ □

A crucial, but less well known property of $\left(\frac{M}{m}\right)$ is the following.

**Proposition 4.** *Suppose* $D \equiv 0, 1 \pmod 4$*. If* $m \equiv n \pmod D$*, then*

$$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right).$$

*Sketch.* For simplicity, we take $D \equiv 1 \pmod 4$, $D > 0$. Then using the quadratic reciprocity law, we have

$$\left(\frac{D}{m}\right) = (-1)^{(D-1)(m-1)/4}\left(\frac{m}{D}\right)$$
$$\left(\frac{D}{n}\right) = (-1)^{(D-1)(n-1)/4}\left(\frac{n}{D}\right).$$

Since $m \equiv n \pmod D$, the Jacobi symbols on the right hand sides agree: $\left(\frac{m}{D}\right) = \left(\frac{n}{D}\right)$. Then we have $(D-1)(m-1)/4 = (D-1)(n-1)/4$, since $D \equiv 1 \pmod 4$, and $m, n$ are odd. So the signs are both $+1$, giving equality.

More generally, for $D < 0$, or $D \equiv 0 \pmod 4$, one can use the supplementary laws to prove the result. □

## Application of Jacobi symbol to quadratic residues

Using the Jacobi symbol, one can compute more efficiently whether or not a $a$ is a quadratic residue modulo a prime $p$. One does not have to factor the numerator before applying quadratic reciprocity.

**Example 5.** Given that 53 is prime, compute $\left(\frac{30}{53}\right)$ and determine whether 30 is a square modulo 53.

Using the Legendre symbol, we have to factor $30 = 2 \times 3 \times 5$, and compute

$$\left(\frac{30}{53}\right) = \left(\frac{2}{53}\right)\left(\frac{3}{53}\right)\left(\frac{5}{53}\right).$$

Then one has to use quadratic reciprocity to 'flip' the symbols (or to evaluate $\left(\frac{2}{53}\right)$), to obtain

$$
\begin{aligned}
&= (-1)^{(53^2-1)/8}(-1)^{(53-1)(3-1)/4}(-1)^{(53-1)(5-1)/4}\left(\frac{53}{3}\right)\left(\frac{53}{5}\right) \\
&= -\left(\frac{53}{3}\right)\left(\frac{53}{5}\right) \\
&= -1 \times -1 \times -1 = -1
\end{aligned}
$$

Thus 30 is not a square modulo 53.

Using the Jacobi symbol, we can directly apply quadratic reciprocity, after removing factors of 2, to obtain

$$
\begin{aligned}
\left(\frac{30}{53}\right) &= \left(\frac{2}{53}\right)\left(\frac{15}{53}\right) \\
&= (-1)^{(53^2-1)/8}(-1)^{(15-1)(53-1)/4}\left(\frac{53}{15}\right) \\
&= \left(\frac{8}{15}\right)
\end{aligned}
$$

Apply quadratic reciprocity again, to get

$$
\begin{aligned}
&= \left(\frac{2}{15}\right)^3 \\
&= (-1)^{3(15^2-1)/8} = -1
\end{aligned}
$$

This leads to an efficient 'Euclidean-style' algorithm for computing $\left(\frac{a}{p}\right)$, without having to factorise $a$ into primes first.

However, one much take care when 'interpreting' the Jacobi symbol $\left(\frac{M}{m}\right) = 1$.

**Remark 6.** We certainly have that $M \equiv \square \pmod{m}$ implies that $\left(\frac{M}{m}\right) = 1$, since $M \equiv \square \pmod{p_i}$ for every prime divisor $p_i$ of $m$. However, the reverse implication does not hold generally; but if $m = p$ is prime, then the Jacobi symbol $\left(\frac{M}{p}\right)$ reduces to the Legendre symbol $\left(\frac{M}{p}\right)$, where this does hold.

For example:

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)^2 = 1\,,$$

but the squares modulo 15 are $0, (\pm1)^2, (\pm2)^2, \cdots, (\pm7)^2 \equiv 0, 1, 4, 6, 9, 10 \pmod{15}$.

## Proof of the lemma

From Proposition 4 it follows that $\chi([m]) := \left(\frac{D}{m}\right)$ is a well-defined function $(\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$, as we can choose a representative $[m]$ so that $m$ is odd and positive. The multiplicative properties above, show that it is a group homomorphism.

Requiring that $\chi([p]) = \left(\frac{D}{p}\right)$ for a prime $p$ fixes $\chi$ uniquely: Dirichlet's theorem on primes in arithmetic progressions tells us that every class $[b] \in (\mathbb{Z}/a\mathbb{Z})^*$ contains some prime $p \equiv b \pmod{a}$.

Moreover, one can check that

$$\chi([-1]) = \begin{cases} 1 & \text{if } D > 0 \\ -1 & \text{if } D < 0 \end{cases}$$