LECTURE 10: JACOBI SYMBOL

1. The Jacobi symbol

We wish to generalise the Legendre symbol $\left(\frac{\cdot}{p}\right)$ to accomodate composite moduli.

Definition 1.1. Let Q be an odd positive integer, and suppose that $Q = p_1 \cdots p_s$, where the p_i are prime numbers (not necessarily distinct). Then we define the **Jacobi symbol** $\left(\frac{a}{Q}\right)$ as follows:

(i) $\left(\frac{a}{1}\right) = 1$;

(ii) $\left(\frac{a}{Q}\right) = 0$ whenever $(a, Q) > 1$;

(iii) $\left(\frac{a}{Q}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right)$ whenever $(a, Q) = 1$.

Just as in the discussion concerning the Legendre symbol, we begin with some simple properties of the Jacobi symbol.

Theorem 1.2. *Suppose that Q and Q' are odd positive integers. Then:*
(i) $\left(\frac{P}{Q}\right)\left(\frac{P}{Q'}\right) = \left(\frac{P}{QQ'}\right)$;
(ii) $\left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right) = \left(\frac{PP'}{Q}\right)$;
(iii) whenever $(P, Q) = 1$, *one has* $\left(\frac{P}{Q^2}\right) = \left(\frac{P^2}{Q}\right) = 1$;
(iv) whenever $(PP', QQ') = 1$, *one has* $\left(\frac{P'P^2}{Q'Q^2}\right) = \left(\frac{P'}{Q'}\right)$;
(v) whenever $P \equiv P' \pmod{Q}$, *one has* $\left(\frac{P}{Q}\right) = \left(\frac{P'}{Q}\right)$.

Proof. Part (i) is immediate from the definition of the Jacobi symbol, and part (ii) is immediate from the properties of the Legendre symbol. Parts (iii) and (iv) follow directly from parts (i) and (ii), since the Jacobi symbol takes values 0 or ± 1. For part (v) of the theorem, observe that whenever $P \equiv P'$ $\pmod{Q}$, one has $P \equiv P' \pmod{p}$ for each prime number p dividing Q, whence also $\left(\frac{P}{p}\right) = \left(\frac{P'}{p}\right)$ for each prime p dividing Q. The desired conclusion is therefore again immediate from the definition of the Jacobi symbol. □

Note 1.3. If the Jacobi symbol $\left(\dfrac{a}{Q}\right) = -1$, then it follows that a is **not** a quadratic residue modulo Q, since for some prime p with $p \mid Q$ one must have that the Legendre symbol $\left(\dfrac{a}{p}\right) = -1$. **But** if $\left(\dfrac{a}{Q}\right) = 1$, then it is **not** necessarily the case that a is a quadratic residue modulo Q. For example, one has

$$\left(\frac{2}{15}\right) = 1, \quad \text{but} \quad \left(\frac{2}{3}\right) = -1 \quad \text{and} \quad \left(\frac{2}{5}\right) = -1.$$

The Jacobi symbol remains useful for calculating Legendre symbols, because it satisfies the same reciprocity and simplifying relations as the Legendre symbol (as we now demonstrate), and at the same time, whenever the Legendre symbol $\left(\dfrac{a}{Q}\right)$ is defined (that is, provided that Q is an odd prime number), then its value is the same as that of the corresponding Jacobi symbol.

Theorem 1.4. *Suppose that Q is an odd positive integer. Then*

$$\left(\frac{-1}{Q}\right) = (-1)^{(Q-1)/2} \quad \textit{and} \quad \left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8}.$$

Proof. Suppose that Q is odd, and that $Q = p_1 \dots p_s$ with each p_i a prime number. Then

$$\left(\frac{-1}{Q}\right) = \prod_{i=1}^{s} \left(\frac{-1}{p_i}\right) = \prod_{i=1}^{s} (-1)^{(p_i-1)/2}.$$

But whenever n_1 and n_2 are both odd, one has $\frac{1}{2}(n_1-1)(n_2-1) \equiv 0 \pmod 2$, whence

$$\tfrac{1}{2}(n_1-1)+\tfrac{1}{2}(n_2-1) = \tfrac{1}{2}(n_1n_2-1)-\tfrac{1}{2}(n_1-1)(n_2-1) \equiv \tfrac{1}{2}(n_1n_2-1) \pmod 2.$$

Iterating the latter relation, we deduce that

$$\tfrac{1}{2}(Q-1) \equiv \sum_{i=1}^{s} \tfrac{1}{2}(p_i-1) \pmod 2,$$

whence $\left(\dfrac{-1}{Q}\right) = (-1)^{(Q-1)/2}$.

Similarly, we have

$$\left(\frac{2}{Q}\right) = \prod_{i=1}^{s} \left(\frac{2}{p_i}\right) = \prod_{i=1}^{s} (-1)^{(p_i^2-1)/8}.$$

But whenever n_1 and n_2 are both odd, it follows that

$$\tfrac{1}{8}(n_1^2-1)(n_2^2-1) \equiv 0 \pmod 2,$$

whence

$$\begin{aligned} \tfrac{1}{8}(n_1^2-1)+\tfrac{1}{8}(n_2^2-1) &= \tfrac{1}{8}(n_1^2n_2^2-1)-\tfrac{1}{8}(n_1^2-1)(n_2^2-1) \\ &\equiv \tfrac{1}{8}(n_1^2n_2^2-1) \pmod 2. \end{aligned}$$

Thus, again iterating this relation, we find that

$$\frac{Q^2-1}{8} \equiv \sum_{i=1}^{s} \frac{p_i^2-1}{8} \pmod 2,$$

whence

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

□

Theorem 1.5 (Quadratic Reciprocity)**.** *Suppose that P and Q are odd positive integers with $(P,Q)=1$. Then*

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

Proof. Suppose that $Q = q_1 \cdots q_s$ and $P = p_1 \cdots p_r$ are factorisations of P and Q, respectively, into products of prime numbers. Then we have

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right).$$

Then by quadratic reciprocity for the Legendre symbol, we obtain

$$\left(\frac{P}{Q}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{(p_i-1)(q_j-1)/4}\left(\frac{q_j}{p_i}\right) = (-1)^{\omega}\left(\frac{Q}{P}\right),$$

where we write

$$\omega = \sum_{i=1}^{r}\sum_{j=1}^{s}\frac{(p_i-1)(q_j-1)}{4}.$$

But as in the proof of Theorem 1.4, one has

$$\begin{aligned}\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{(p_i-1)(q_j-1)}{4} &= \left(\sum_{i=1}^{r}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\right)\\ &\equiv \tfrac{1}{2}(P-1)\cdot\tfrac{1}{2}(Q-1) \pmod 2.\end{aligned}$$

We therefore deduce that

$$\left(\frac{P}{Q}\right) = (-1)^{(P-1)(Q-1)/4}\left(\frac{Q}{P}\right),$$

and the conclusion of the theorem now follows immediately. □

Jacobi symbols are useful for calculating Legendre symbols, since they take the same values for prime moduli, and one can skip intermediate factorisations before applying reciprocity.

Example 1.6. Calculate the Legendre symbol $\left(\frac{1111}{8093}\right)$.

One has

$$\begin{aligned}\left(\frac{1111}{8093}\right) &= (-1)^{(1110)(8092)/4}\left(\frac{8093}{1111}\right) = \left(\frac{316}{1111}\right) = \left(\frac{2}{1111}\right)^2\left(\frac{79}{1111}\right)\\ &= (-1)^{(78)(1110)/4}\left(\frac{1111}{79}\right) = -\left(\frac{5}{79}\right) = -(-1)^{(4)(78)/4}\left(\frac{79}{5}\right)\\ &= -\left(\frac{4}{5}\right) = -\left(\frac{2}{5}\right)^2 = -1.\end{aligned}$$

So 1111 is not a quadratic residue modulo 8093.

Example 1.7. Determine whether or not the congruence $x^2 + 6x - 50 \equiv 0 \pmod{79}$ has a solution.

Observe that $x^2+6x-50 = (x+3)^2-59$, and hence $x^2+6x-50 \equiv 0 \pmod{79}$ has a solution if and only if $\left(\frac{59}{79}\right) = 1$. But

$$\begin{aligned}\left(\frac{59}{79}\right) &= \left(\frac{-20}{79}\right) = \left(\frac{-1}{79}\right)\left(\frac{2}{79}\right)^2\left(\frac{5}{79}\right) = (-1)^{(79-1)/2}\left(\frac{5}{79}\right)\\ &= -(-1)^{(5-1)(79-1)/4}\left(\frac{79}{5}\right) = -\left(\frac{4}{5}\right) = -1.\end{aligned}$$

Hence the congruence $x^2 + 6x - 50 \equiv 0 \pmod{79}$ has no solution.

Example 1.8. Let p be an odd prime. Compute $\sum_{x=1}^{p}\left(\frac{x}{p}\right)$.

Let $S = \sum_{x=1}^{p}\left(\frac{x}{p}\right)$. There exists a such that $\left(\frac{a}{p}\right) = -1$. For instance, this is the case when a is a primitive root modulo p because of Euler's criterion. Since $(a,p) = 1$, the map $x \mapsto ax \pmod{p}$ defines a bijection on the set of residues modulo p. So

$$S = \sum_{x=1}^{p}\left(\frac{ax}{p}\right) = \sum_{x=1}^{p}\left(\frac{a}{p}\right)\left(\frac{x}{p}\right) = -S.$$

Hence, $S = 0$.

2. Counting solutions of congruences

For an odd prime p and $a, b, c \in \mathbb{Z}$ with $(a,p) = 1$, we consider the congruence

$$y^2 \equiv ax^2 + bx + c \pmod{p} \tag{2.1}$$

Let $D = b^2 - 4ac$ be the discriminant.

Theorem 2.1. *The number of solutions with $1 \leqslant x, y \leqslant p$ of (2.1) is equal to:*

- $p - \left(\frac{a}{p}\right)$ *if $p \nmid D$,*
- $p + (p-1)\left(\frac{a}{p}\right)$ *if $p \mid D$.*

Proof. We observe that the number of solutions can be represented as the sum

$$\sum_{x=1}^{p}\left(1+\left(\frac{ax^2+bx+c}{p}\right)\right)=p+\sum_{x=1}^{p}\left(\frac{ax^2+bx+c}{p}\right).$$

We observe that

$$4a(ax^2+bx+c)=(2ax+b)^2-D,$$

Since the map $x\mapsto 2ax+b \pmod p$ defines a bijection on the set of residues modulo p, we obtain

$$\begin{aligned}\sum_{x=1}^{p}\left(\frac{ax^2+bx+c}{p}\right)&=\sum_{x=1}^{p}\left(\frac{(4a)^{-1}}{p}\right)\left(\frac{(2ax+b)^2-D}{p}\right)\\&=\left(\frac{(4a)^{-1}}{p}\right)\sum_{y=1}^{p}\left(\frac{y^2-D}{p}\right).\end{aligned}$$

By the properties of Legendre symbol,

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

We write

$$S(D)=\sum_{y=1}^{p}\left(\frac{y^2-D}{p}\right).$$

Then the number of solutions is $p+\left(\frac{a}{p}\right)S(D)$.

When $p|D$,

$$S(D)=\sum_{y=1}^{p}\left(\frac{y^2}{p}\right)=p-1.$$

This immediately implies the second part of the theorem.

Suppose then that $p\nmid D$. We observe that

$$S(D)=\left(\frac{-D}{p}\right)+2\sum_{1\leqslant z\leqslant p}{}^{*}\left(\frac{z-D}{p}\right),$$

where the sum is carried out over all non-zero quadratic residues z. We can also rewrite this formula as

$$S(D)=\sum_{z=1}^{p}\left(\left(\frac{z}{p}\right)+1\right)\left(\frac{z-D}{p}\right).$$

Consider the map $z \mapsto \bar{z}$ such that $\bar{p} = p$ and $\bar{z}$ satisfies $z\bar{z} \equiv 1 \pmod{p}$. Then $\left(\frac{z}{p}\right) = \left(\frac{\bar{z}}{p}\right)$, and

$$\begin{aligned} S(D) &= \sum_{z=1}^{p} \left(\left(\frac{\bar{z}}{p}\right) + 1\right) \left(\frac{z-D}{p}\right) = \sum_{z=1}^{p} \left(\frac{\bar{z}z - D\bar{z}}{p}\right) + \sum_{z=1}^{p} \left(\frac{z-D}{p}\right) \\ &= \sum_{z=1}^{p-1} \left(\frac{1-D\bar{z}}{p}\right) + \sum_{z=1}^{p} \left(\frac{z-D}{p}\right) \\ &= -1 + \sum_{z=1}^{p} \left(\frac{1-D\bar{z}}{p}\right) + \sum_{z=1}^{p} \left(\frac{z-D}{p}\right) \end{aligned}$$

Since the map $z \mapsto 1 - D\bar{z} \pmod{p}$ defines a bijection, we obtain

$$\sum_{z=1}^{p} \left(\frac{1-D\bar{z}}{p}\right) = \sum_{x=1}^{p} \left(\frac{x}{p}\right),$$

and similarly,

$$\sum_{z=1}^{p} \left(\frac{z-D}{p}\right) = \sum_{x=1}^{p} \left(\frac{x}{p}\right).$$

Hence, these sums are zero by Example 1.8. This implies that $S(D) = -1$, which proves the theorem. □