A.6 Quadratic Reciprocity

Quadratic reciprocity provides a very convenient method of computing the Jacobi (or Legendre) symbol and thereby deciding quadratic residuosity. It relies on the following two propositions and a lemma that helps to reduce composite modules to prime modules.

Lemma 15 *Let $s, t \in \mathbb{Z}$ be odd. Then*

(i) $\frac{s-1}{2} + \frac{t-1}{2} \equiv \frac{st-1}{2} \pmod 2$,

(ii) $\frac{s^2-1}{8} + \frac{t^2-1}{8} \equiv \frac{s^2t^2-1}{8} \pmod 2$.

Proof. Assume $s = 2k+1$ and $t = 2l+1$. Then $st = 4kl + 2k + 2l + 1$,

$$\frac{st-1}{2} = 2kl + k + l \;\equiv\; k + l = \frac{s-1}{2} + \frac{t-1}{2}.$$

Moreover

$$\begin{aligned} s^2 = 4 \cdot (k^2+k) + 1, &\quad t^2 = 4 \cdot (l^2 + l) + 1, \\ s^2t^2 &= 16 \cdot \ldots + 4 \cdot (k^2 + k + l^2 + l) + 1, \\ \frac{s^2t^2-1}{8} &= 2 \cdot \ldots + \frac{k^2+k+l^2+l}{2}, \end{aligned}$$

and this proves the assertion. $\diamond$

Proposition 20 *Let n be odd. Then*

(i) $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$,

(ii) $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$

Proof. The lemma reduces the assertions to the case $n = p$ prime.

(i) is a direct consequence of Euler's criterion, Proposition 19.

(ii) We have

$$(-1)^k \cdot k \equiv \begin{cases} k, & \text{if } k \text{ is even}, \\ p-k, & \text{if } k \text{ is odd}, \end{cases}$$

$$\prod_{k=1}^{\frac{p-1}{2}} (-1)^k \cdot k \equiv 2 \cdot 4 \cdots (p-1) = 2^{\frac{p-1}{2}} \cdot (\frac{p-1}{2})!.$$

Om the other hand

$$\prod_{k=1}^{\frac{p-1}{2}} (-1)^k \cdot k = (\frac{p-1}{2})! \cdot (-1)^{\frac{p^2-1}{8}}, \quad \text{since} \quad \sum_{k=1}^{\frac{p-1}{2}} k = \frac{(p-1)(p+1)}{2 \cdot 2 \cdot 2}.$$

Now $(\frac{p-1}{2})!$ is a product of positive integers $< p$, thus not a multiple of p. Hence we may divide by it. Then from the two equations and EULER's criterion we get

$$(-1)^{\frac{p^2-1}{8}} \equiv 2^{\frac{p-1}{2}} \equiv (\frac{2}{p}) \pmod{p}.$$

Since $p \geq 3$ this congruence implies equality. $\diamond$

In particular 2 is a quadratic residue modulo the prime p if and only if $(p^2-1)/8$ is even, or $p^2 \equiv 1 \pmod{16}$, or $p \equiv 1$ or $7 \pmod{8}$.

Theorem 3 (Law of Quadratic Reciprocity) *Let m and n be two different odd coprime positive integers. Then*

$$(\frac{m}{n})(\frac{n}{m}) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Here is a somewhat more comprehensible formula:

$$(\frac{m}{n}) = \begin{cases} -(\frac{n}{m}) & \text{if } m \equiv n \equiv 3 \pmod{4}, \\ (\frac{n}{m}) & \text{else.} \end{cases}$$

The proof is in the next section. First we illustrate the computation with an example:

Is 7 a quadratic residue mod 107? *No*, as the following computation shows:

$$(\frac{7}{107}) = -(\frac{107}{7}) = -(\frac{2}{7}) = -1.$$

Likewise 7 is not a quadratic residue mod 11:

$$(\frac{7}{11}) = -(\frac{11}{7}) = -(\frac{4}{7}) = -(\frac{2}{7})(\frac{2}{7}) = -1.$$

Hence 7 is a quadratic non-residue also mod $1177 = 11 \cdot 107$. But $(\frac{7}{1177}) = 1$.

From the law of quadratic reciprocity we derive the following algorithm:

Procedure JacobiSymbol

Input parameters:
  m, n = two integers.
Output parameter:
  jac $= (\frac{m}{n})$.
Instructions:
  If $n = 0$ output jac $= 0$ **end**
  If $m = 0$ output jac $= 0$ **end**
  If $\gcd(m, n) > 1$ output jac $= 0$ **end**
  [*Now* $m, n \neq 0$ *are coprime, so jac* $= \pm 1$.]
  jac $= 1$.
  If $n < 0$ replace n by $-n$.
  If n is even divide n by the maximum possible power 2^k.
  If $m < 0$
    replace m by $-m$,
    if $n \equiv 3 \pmod 4$ replace jac by $-$jac.
  [*From now on* m *and* n *are coprime, and* n *is positive and odd.*]
  [*In the last step* $m = 0$ *and* $n = 1$ *may occur.*]
  If $m > n$ replace m by $m \bmod n$.
  While $n > 1$:
    If m is even:
      Divide m by the maximum possible power 2^k,
      if (k is odd and $n \equiv \pm 3 \pmod 8$) replace jac by $-$jac.
    [*Now* m *and* n *are odd and coprime,* $0 < m < n$.]
    [*The law of quadratic reciprocity applies.*]
    If ($m \equiv 3 \pmod 4$ and $n \equiv 3 \pmod 4$)
      replace jac by $-$jac.
    Set $d = m$, $m = n \bmod m$, $n = d$.

The analysis of this algorithm resembles the analysis of the Euclidean algorithm: We need at most $5 \cdot \log(m)$ steps, each one essentially consisting of one integer division. Since the size of the operands rapidly decreases, the total cost amounts to $\mathrm{O}(\log_2(m)^2)$. This is significantly faster than applying Euler's criterion.