YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467a: Cryptography and Computer Security *Handout #6*
Professor M. J. Fischer *September 29, 2005*

The Legendre and Jacobi Symbols

Let $a \geq 0, n \in \mathbf{Z}^+$. Let $\mathrm{QR}(a,n)$ hold if $(a,n) = 1$ and a is a quadratic residue modulo n. Let $\mathrm{QNR}(a,n)$ hold if $(a,n) = 1$ and a is a quadratic non-residue modulo n (i.e., there is no $y \in \mathbf{Z}_n^*$ such that $a \equiv y^2 \pmod{n}$).

For a prime p, the structure of quadratic residues can be fairly easily explained. Let g be a primitive root of $\mathbf{Z}_p^*$. Then every element of $\mathbf{Z}_p^*$ is uniquely expressible as g^k for some $k \in \{0, \ldots, p-2\}$.

Theorem 1 *Let p be a prime, g a primitive root of p, $a \equiv g^k \pmod{p}$. Then a is a quadratic residue iff k is even.*

Proof: If k is even, then $g^{k/2}$ is easily seen to be a square root of a modulo p.

Conversely, suppose $a \equiv y^2 \pmod{p}$. Write $y \equiv g^\ell \pmod{p}$. Then $g^k \equiv g^{2\ell} \pmod{p}$. Multiplying both sides by g^{-k}, we have $1 \equiv g^0 \equiv g^{2\ell-k} \pmod{p}$. But then $\phi(p) \,|\, 2\ell - k$. Since $2 \,|\, \phi(p) = p-1$, it follows that $2 \,|\, k$, as desired. ■

The following theorem, due to Euler, is now easily proved:

Theorem 2 (Euler) *Let p be an odd prime, and let $a \geq 0$, $(a,p) = 1$. Then*

$$a^{(p-1)/2} \equiv \begin{cases} 1 \pmod{p} & \text{if } \mathrm{QR}(a,p) \text{ holds;} \\ -1 \pmod{p} & \text{if } \mathrm{QNR}(a,p) \text{ holds.} \end{cases}$$

Proof: Write $a \equiv g^k \pmod{p}$.

If $\mathrm{QR}(a,p)$ holds, then a is a quadratic residue modulo p, so k is even by Theorem 1. Write $k = 2r$ for some r. Then $a^{(p-1)/2} \equiv g^{2r(p-1)/2} \equiv (g^r)^{p-1} \equiv 1 \pmod{p}$ by Fermat's theorem.

If $\mathrm{QNR}(a,p)$ holds, then a is a quadratic non-residue modulo p, so k is odd by Theorem 1. Write $k = 2r+1$ for some r. Then $a^{(p-1)/2} \equiv g^{(2r+1)(p-1)/2} \equiv g^{r(p-1)} g^{(p-1)/2} \equiv g^{(p-1)/2} \pmod{p}$. Let $b = g^{(p-1)/2}$. Clearly $b^2 \equiv 1 \pmod{p}$, so $b \equiv \pm 1 \pmod{p}$.[1] Since g is a primitive root modulo p and $(p-1)/2 < p-1$, $b = g^{(p-1)/2} \not\equiv 1 \pmod{p}$. Hence, $b \equiv -1 \pmod{p}$. ■

Definition: The Legendre symbol is a function of two integers a and p, written $\left(\frac{a}{p}\right)$. It is defined for $a \geq 0$ and p an odd prime as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } \mathrm{QR}(a,p) \text{ holds;} \\ -1 \text{ if } \mathrm{QNR}(a,p) \text{ holds;} \\ 0 \text{ if } (a,p) \neq 1. \end{cases}$$

A multiplicative property of the Legendre symbols follows immediately from Theorem 1.

Observation 3 *Let $a, b \geq 0$, p an odd prime. Then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

[1] This follows from the fact that $p | (b^2 - 1) = (b-1)(b+1)$, so either $p \,|\, (b-1)$, in which case $b \equiv 1 \pmod{p}$, or $p \,|\, (b+1)$, in which case $b \equiv -1 \pmod{p}$.

As an easy corollary of Theorem 2, we have:

Corollary 4 *Let $a \geq 0$ and let p be an odd prime. Then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

The Jacobi symbol extends the domain of the Legendre symbol.

Definition: The Jacobi symbol is a function of two integers a and n, written $\left(\frac{a}{n}\right)$, that is defined for all $a \geq 0$ and all odd positive integers n. Let $\prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization of n. Then

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

Here $\left(\frac{a}{p_i}\right)$ denotes the previously-defined Legendre symbol. (Note that by this definition, $\left(\frac{0}{1}\right) = 1$, and $\left(\frac{0}{n}\right) = 0$ for odd $n \geq 3$.)

We have seen that if $(a, p) = 1$ and p is prime, then the Legendre symbol $\left(\frac{a}{p}\right) = 1$ iff a is a quadratic residue modulo p. It is *not* true for the Jacobi symbol that $\left(\frac{a}{n}\right) \equiv 1 \pmod{n}$ implies that a is a quadratic residue modulo n. For example, $\left(\frac{8}{15}\right) = 1$, but 8 is not a quadratic residue modulo 15. However, the converse does hold:

Observation 5 *If $\left(\frac{a}{n}\right) \not\equiv 1 \pmod{n}$, then a is not a quadratic residue modulo n.*

The usefulness of the Jacobi symbol $\left(\frac{a}{n}\right)$ stems from its ability to be computed efficiently, even without knowning the factorization of either a or n. The algorithm is based on the following theorem, which is stated without proof.

Theorem 6 *Let n be an odd positive integer, $a, b \geq 0$. Then the following identities hold:*

(a) $$\left(\frac{0}{n}\right) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n > 1 \end{cases}$$

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

(c) $$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right) \text{ if } a \equiv b \pmod{n}.$$

(d) $$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$$

(e) (Quadratic reciprocity). If a is odd, then
$$\left(\frac{a}{n}\right) = \begin{cases} -\left(\frac{n}{a}\right) & \text{if } a \equiv n \equiv 3 \pmod{4}; \\ \left(\frac{n}{a}\right) & \text{otherwise.} \end{cases}$$

Theorem 6 leads directly to a recursive algorithm for computing $\left(\frac{a}{n}\right)$:

```
int jacobi(int a, int n)
/* Precondition: a, n >= 0; n is odd */
{
  int ans;

  if (a == 0)
    ans = (n==1) ? 1 : 0;
  else if (a == 2) {
    switch (n%8) {
    case 1:
    case 7:
      ans = 1;
      break;
    case 3:
    case 5:
      ans = -1;
      break;
    }
  }
  else if ( a >= n )
    ans = jacobi(a%n, n);
  else if (a%2 == 0)
    ans = jacobi(2,n)*jacobi(a/2, n);
  else
    ans = (a%4 == 3 && n%4 == 3) ? -jacobi(n,a) : jacobi(n,a);
  return ans;
}
```