Jacobi Symbol and its computation

Barbarino Giovanni

July 19, 2015

Abstract

A short essay on the methods of computation of the Legendre and Jacobi-Kronecker Symbol

Contents

1 Legendre Symbol

One of the problem that aroused in algebra was to determine, taken p an odd prime, and $0 \leq a < p$ an integer, if the equation

$$x^2 \equiv a \pmod{p}$$

has any solution in $\mathbb{Z}/p\mathbb{Z}$ and how many they are.

Since the group $\mathbb{Z}/p\mathbb{Z}$ is a field, from the Fundamental Theorem of Algebra we know that $x^2 - a = 0$ has two solutions in an algebraic closure. Moreover, if $b \in (\mathbb{Z}/p\mathbb{Z})^*$ is a solution, then also $-b$ is a solution, and $b \neq -b$ since p is odd.
From this observations, we deduce there are only three cases:

$$\begin{cases} \text{2 distinct solutions} & \text{if } \exists b \neq 0 : b^2 = a \\ \text{1 solution} & \text{if } a = 0 \\ \text{no solutions} & \text{if } \nexists b : b^2 = a \end{cases}$$

In the first case, we say that a is a *quadratic residue* modulus p, and in the last case we say that a is not a quadratic residue.
If $p = 2$ we have

$$x^2 - a \equiv (x-a)^2 \pmod{2}$$

so it's easy to find solutions.

We can now define the *Legendre Symbol*

Definition 1. Given p an odd positive prime, and a an integer, we define the **Legendre Symbol** as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \pmod{p} \\ 1 & \exists\, x : a \equiv x^2 \pmod{p} \\ -1 & \text{otherwise} \end{cases}$$

We know that, if p is prime, there exists a generator g of the group $(\mathbb{Z}/p\mathbb{Z})^*$. It's obvious that if $a = g^{2n}$ then a is a quadratic residue, so $\left(\frac{a}{p}\right) = 1$. We can also prove that this condition is necessary and sufficient:

Lemma 1. *The Legendre symbol can be computed as*

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

Proof. We can always suppose $0 \leq a \leq p-1$. If $a = 0$, then it's obvious.
If g is the generator of $(\mathbb{Z}/p\mathbb{Z})^*$, then $a \neq 0$ is a quadratic residue if and only if there exists $x \neq 0 : x^2 = a$, so

$$\left(\frac{a}{p}\right) = 1 \iff \exists x \neq 0 : x^2 = a \iff \exists m : (g^m)^2 = g^{2m} = a$$

since $p-1$ is even, then it also means that $a \neq 0$ is not a quadratic residue if and only if is an odd power of g.
We know that $g^{(p-1)/2} = -1$, since it's a root of $x^2 - 1$ and it's different from 1.
If a is a quadratical residue, then

$$a = g^{2n} \implies a^{(p-1)/2} = g^{n(p-1)} = 1$$

If a is not a quadratical residue, then

$$a = g^{2n+1} \implies a^{(p-1)/2} = g^{n(p-1)} g^{(p-1)/2} = -1$$

□

This gives us a simple way of computing the Legendre Symbol: given a and p, we have

```
**if** $a = 0$ **then return** 0
**end if**
$y = 1$ , $n = (p-1)/2$
**while** $n \neq 0$ **do**
    **if** $n$ odd **then**
        $y = y * a \pmod{p}$
        $n = n - 1$
    **else**
        $a = a * a \pmod{p}$
        $n = n/2$
    **end if**
**end while**
**return** $y$
```

This algorithm runs in $O(\log^3(p))$ due to the cost of the multiplications. We can do better, but we need some other property of the Legendre Symbol.

First of all we can prove that it's multiplicative on a:

Lemma 2. *The Legendre Symbol is multiplicative on a, that is*

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

Proof. Using the result above,

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

□

The most important theorem on this symbol is called *Legendre-Gauss quadratic reciprocity law*, that is not so simple to prove as the precedent propositions:

Theorem 2. *Given p and q different old primes, and $a \neq 0 \pmod p$, then*

1.

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

where μ is the number of values in $\{a, 2a, 3a, \ldots, (p-1)a/2\}$ such that their residues modulus p are greater than $p/2$

2. If $a = q$, and $p' = (p-1)/2$, then

$$\sum_{k=1}^{p'} \left\lfloor \frac{kq}{p} \right\rfloor \equiv \mu \pmod 2$$

3.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

Proof.

1. the residues of $\{a, 2a, 3a, \ldots, (p-1)a/2\}$ are all different among them, and we call them

$$r_1, r_2, \ldots, r_\lambda \qquad -r'_1, -r'_2, \ldots, -r'_\mu$$

$$\lambda + \mu = (p-1)/2, \qquad 0 < r_i < p/2, \qquad 0 < r'_i < p/2$$

If $r_i = r'_j$, then, modulus p,

$$ma = r_i \qquad na = -r'_j \implies ma + na = 0 \implies m + n = 0$$

which is impossible. So r_i and r'_i are a rearrangement of $1, \ldots, (p-1)/2$, and

$$a^{(p-1)/2}\left[\frac{p-1}{2}\right]! \equiv a \cdot 2a \cdot \cdots \cdot (p-1)a/2 \equiv (-1)^{\mu}\left[\frac{p-1}{2}\right]!$$

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

2. Given $\{q, 2q, 3q, \dots, p'q\}$, we can write
$$kq = p\left\lfloor \frac{kq}{p} \right\rfloor + u_k \tag{1}$$
where $1 \le k \le p' \implies 0 < u_k < p$. We have, like above, that we can divide u_k into
$$r_1, r_2, \dots, r_\lambda \qquad -r'_1, -r'_2, \dots, -r'_\mu$$
$$\lambda + \mu = p', \qquad 0 < r_i < p/2, \qquad 0 < r'_i < p/2,$$
and we define $w_i = -r'_i + p$ that correspond to $u_i > p/2$.
Let's sum the equation (1) for all k until it reaches p'. The sum of numbers from 1 to p' is $(p^2-1)/8$, so
$$q\frac{p^2-1}{8} = p\sum\left\lfloor \frac{kq}{p} \right\rfloor + \sum u_k = p\sum\left\lfloor \frac{kq}{p} \right\rfloor + \sum r_i + \sum w_i$$
$$\sum r_i + \sum r'_i = \frac{p^2-1}{8} \implies \mu p + \sum r_i - \sum w_i = \frac{p^2-1}{8}$$
$$\implies q\frac{p^2-1}{8} = p\sum\left\lfloor \frac{kq}{p} \right\rfloor + 2\sum w_i + \frac{p^2-1}{8} - \mu p$$
$$\implies (q-1)\frac{p^2-1}{8} = p\sum\left\lfloor \frac{kq}{p} \right\rfloor + 2\sum w_i - \mu p$$
but $q-1$ is even, p^2-1 is divisible by 8, and p is odd, so
$$\sum\left\lfloor \frac{kq}{p} \right\rfloor \equiv \mu \pmod 2$$

3. Let's call $p' = (p-1)/2$, and $q' = (q-1)/2$. If we call $S(q,p)$ the quantity above, we have that
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)}$$
The last step is to prove that $S(p,q) + S(q,p) = p'q'$. Let's suppose $p > q$. Given a couple (a,b) with $0 < a, b$, we have
$$b/a < q/p \iff b < aq/p, \qquad b/a > p/q \iff a < bq/p$$
If $a \le p'$, $b \le q'$, then aq/p and bp/q are not integer, so $\lfloor aq/p \rfloor$ is the number of couples (a,b) with $b < aq/p$, but it's easy to verify that $a \le p' \implies b \le q'$ and the same for $\lfloor bp/q \rfloor$. The thesis follow.

□

Using this results, we can device another algorithm. In fact we can factorize a into primes, and apply the reciprocity law on each factor. This algorithm, though, have some big flaws: the factorization is slow, and we could end up with too many factors.

In order to optimize this algorithm, we will introduce the Jacobi-Kronecker Symbol, but before that, we need a last result:

Theorem 3. *Given p an old prime, then*

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

Proof. Let's first suppose that $p \equiv 1 \pmod 4$. Define S as the product of the even values between 1 and $p-1$ modulus p. We can see they are exactly $\{2, 2\cdot 2, 3\cdot 2, \ldots, (p-1)2/2\}$. We notice that, from (Theorem 2), $\mu = (p-1)/4$, and keeping in mind that $(p+1)/2$ is odd, we obtain

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/4} = \left((-1)^{(p-1)/4}\right)^{(p+1)/2} = (-1)^{(p^2-1)/8}$$

The other case is $p \equiv 3 \pmod 4$. Repeating the same argument, and noticing that $\mu = (p+1)/4$ and that $(p-1)/2$ is odd, we obtain

$$\left(\frac{2}{p}\right) = (-1)^{(p+1)/4} = \left((-1)^{(p+1)/4}\right)^{(p-1)/2} = (-1)^{(p^2-1)/8}$$

□

2 Jacobi-Kronecker Symbol

Definition 4. Given a and b two integers, let's define the **Kronecker Symbol** $\left(\frac{a}{b}\right)$ as follows:

- If $b = 0$, then
$$\left(\frac{a}{0}\right) = \begin{cases} 1 & a = \pm 1 \\ 0 & \text{otherwise} \end{cases}$$
- If $b = -1$, then
$$\left(\frac{a}{-1}\right) = \begin{cases} 1 & a \geq 0 \\ -1 & a < 0 \end{cases}$$
- If $b = 2$, then
$$\left(\frac{a}{2}\right) = \begin{cases} 0 & a \text{ even} \\ (-1)^{(a^2-1)/8} & a \text{ odd} \end{cases}$$
- If not in one of the precedent options, we write $b = \prod p$, where p are primes, not necessarily distinct, or $p = -1$. Then
$$\left(\frac{a}{b}\right) = \prod \left(\frac{a}{p}\right)$$

This Symbol is well-defined thanks to the fact that the factorization in $\mathbb{N}$ is unique, so we have only to look out for $b = -1$. In fact, $b = (-1)(-1)b$, but $\left(\frac{a}{-1}\right)^2 = 1$, so there's no problem. More in general, if b is a perfect square different from zero, then $\left(\frac{a}{b}\right) = 1$, so for every b not zero, we can substitute it with his squarefree part.

The main aim for this Symbol is to extend the Legendre Symbol so that it becomes multiplicative even in his lower part, and such that a more generalized reciprocity law holds.

This new Symbol gains a lot of useful properties, such as

Lemma 3. *Given a, b and c integers, we have*

1.
$$\left(\frac{a}{b}\right) = 0 \iff (a, b) \neq 1$$

2. If $c \neq -1$, or $ab \neq 0$,

$$\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$$

3. If $a \neq -1$, or $bc \neq 0$,

$$\left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right)$$

Proof.

1. Obviously, if p is a prime, then

$$p|(a,b) \implies \left(\frac{a}{b}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{b'}\right) = 0$$

Conversely, suppose $(a,b) = 1$ and $\left(\frac{a}{b}\right) = 0$.

$$b \neq 0, \quad (a,b) = 1 \implies \left(\frac{a}{b}\right) = \prod\left(\frac{a}{p}\right) = \pm 1 \qquad \text{absurd}$$

$$b = 0, \quad (a,b) = 1 \implies a = \pm 1, \quad \left(\frac{\pm 1}{0}\right) = 1 \qquad \text{absurd}$$

2. If $c = 0$, then it's pretty obvious. Otherwise, we can factorize c in primes and use the multiplicativity of the Legendre symbol. The only cases that remains to control are $c = -1, 2$, but if $c = -1$ and $ab \neq 0$, then it's also trivial. If $c = 2$ and ab is even, then a or b is even, and the thesis follows. Otherwise, a and b are both odd, and

$$\left(\frac{ab}{2}\right) = (-1)^{(a^2b^2-1)/8} = (-1)^{(a^2-1)(b^2-1)/8+(a^2-1)/8+(b^2-1)/8} = \left(\frac{a}{2}\right)\left(\frac{b}{2}\right)$$

since $(a^2-1)(b^2-1)/8$ is even.
Lastly, if $ab = 0$, and $a = 0$, then $\left(\frac{a}{c}\right) = \left(\frac{ab}{c}\right) = \left(\frac{0}{c}\right)$ and it's different from 0 only if $c = -1$.

3. If $bc \neq 0$, then it's trivial once you factorize b and c. If $bc = 0$, then, without loss of generality, we can say that $b = 0$. If $a \neq \pm 1$, then $\left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right) = 0$ and the proposition holds. Moreover, if $a = 1$, then

$$\left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right) = \left(\frac{1}{0}\right) = 1, \qquad \left(\frac{a}{c}\right) = \left(\frac{1}{c}\right) = 1$$

where the last equality holds for all c integer.

□

The Kronecker Symbol extends the Legendre one, but it doesn't keeps all his properties. For example, given a, b integers, with $b > 1$, and r the residue of a modulus b, it's not true anymore that

$$\left(\frac{a}{b}\right) = \left(\frac{r}{b}\right)$$

In fact, the case $b = 2$ (or in general b even) is where it fails:

$$\left(\frac{3}{2}\right) = -1, \qquad \left(\frac{1}{2}\right) = 1$$

However, there are is a weaker result we can use:

Theorem 5. *Given $b > 0$, then the Kronecker Symbol is periodic in a. In particular*

$$\left(\frac{a}{b}\right) = \begin{cases} \left(\dfrac{a+b}{b}\right) & b \not\equiv 2 \pmod 4 \\ \\ \left(\dfrac{a+4b}{b}\right) & b \equiv 2 \pmod 4 \end{cases}$$

Proof. Factorizing b, the Legendre Symbol is periodic in a of period b, and we have to test only the case 2. If 2 is among the factors of b, then b is even, so the case a even is simple. Moreover, if b has an even number of factors 2, then it's also easy, so we are in one of the following 2 cases: $b \equiv 2 \pmod 4$ or $8|b$. Let's suppose a odd and $b = 2b'$:

$$\left(\frac{a+b}{2}\right) = (-1)^{((a+b)^2-1)/8} = \left(\frac{a}{2}\right)(-1)^{(2ab+b^2)/8} = \left(\frac{a}{2}\right)(-1)^{b'(a+b')/2}$$

If $8|b$, then $(-1)^{b'(a+b')/2} = 1$, so the only case not tested is $b \equiv 2 \pmod 4$. In this case, the same result may not hold, but

$$\left(\frac{a+4b}{2}\right) = (-1)^{((a+4b)^2-1)/8} = \left(\frac{a}{2}\right)(-1)^{2ab'+8b'^2} = \left(\frac{a}{2}\right)$$

□

Once we have fixed the periodicity, we can now get to proving the reciprocity law, but for its proof, we need some intermediate propositions, and two crucial observations: if a and b are odd, then

$$\frac{ab-1}{2} = \frac{(a-1)(b-1)+(a-1)+(b-1)}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2$$

and we also have

$$\left(\frac{a}{-1}\right) = sgn(a) = (-1)^{(sgn(a)-1)/2}$$

where $sgn(0) = 1$.

Lemma 4.

1. *Given an integer n, then*
$$\left(\frac{n}{0}\right) = \left(\frac{0}{n}\right)$$

2. *Given an integer n, then*
$$\left(\frac{n}{2}\right) = \left(\frac{2}{n}\right)$$

3. *Given an integer $n \neq 0$, such that $n = \pm 2^s n'$ with n' odd and positive,*
$$\left(\frac{n}{-1}\right) = \left(\frac{-1}{n}\right)(-1)^{(n'-1)/2}$$

Proof.

1. It's trivial

2. Let's divide it into cases. If $n = 0, 2$ or -1 then it's pretty obvious. If $n = p$ is an odd prime, then by (Theorem 1) and the definition,
$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \left(\frac{p}{2}\right)$$
If n is a generic integer, then we conclude by multiplicativity
$$\left(\frac{n}{2}\right) = \prod \left(\frac{p}{2}\right) = \prod \left(\frac{2}{p}\right) = \left(\frac{2}{n}\right)$$

3. It's easy with $n = -1, 2$. If $n = p$ is a positive prime, then
$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{(p-1)/2}\left(\frac{p}{-1}\right)$$
We conclude by multiplicativity and the observation above
$$\left(\frac{n}{-1}\right) = \left(\frac{\pm 2^s}{-1}\right)\prod\left(\frac{p}{-1}\right) = \left(\frac{-1}{\pm 2^s}\right)\prod\left(\frac{-1}{p}\right)(-1)^{\sum (p-1)/2} =$$
$$= \left(\frac{-1}{n}\right)(-1)^{\sum (p-1)/2} = \left(\frac{-1}{n}\right)(-1)^{(n'-1)/2}$$

□

We can now state the *generalized quadratic reciprocity law*

Theorem 6. *Given two odd integers a, b, such that a or b is positive, then we have*
$$\left(\frac{a}{b}\right) = (-1)^{(a-1)(b-1)/4}\left(\frac{b}{a}\right)$$

Proof. First of all, $(a, b) \neq 1$ if and only if both the symbols in the formulas are zero, so from now on, we will consider a, b coprimes. If b or a was 1, then it would be pretty obvious. If a (or b) were -1, by (Lemma 3) we have

$$\left(\frac{b}{a}\right) = \left(\frac{b}{-1}\right) = \left(\frac{-1}{b}\right)(-1)^{(b-1)/2} = \left(\frac{a}{b}\right)(-1)^{(a-1)(b-1)/4}$$

Let's suppose $|a|$ and $|b|$ greater then 1.
In the case where a, b were positive, then $\quad a = \prod p, \quad b = \prod q$

$$\left(\frac{a}{b}\right) = \prod_{p,q}\left(\frac{p}{q}\right) = \prod_{p,q}\left(\frac{q}{p}\right)(-1)^{\sum \frac{p-1}{2} \sum \frac{q-1}{2}} = \left(\frac{b}{a}\right)(-1)^{(a-1)(b-1)/4}$$

If $b < 0$, $a > 0$, then

$$\left(\frac{a}{b}\right) = \left(\frac{a}{-b}\right) = \left(\frac{-b}{a}\right)(-1)^{(a-1)(-b-1)/4} = \left(\frac{b}{a}\right)(-1)^{(a-1)/2}(-1)^{(a-1)(-b-1)/4}$$

$$= \left(\frac{b}{a}\right)(-1)^{(a-1)(1-b)/4} = \left(\frac{b}{a}\right)(-1)^{(a-1)(b-1)/4}$$

the same reasoning holds for $b > 0$, $a < 0$. □

In particular, if b is odd and positive, and a is odd, then

$$\left(\frac{a}{b}\right) = (-1)^{(a-1)(b-1)/4}\left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/4}\left(\frac{b}{|a|}\right)$$

so we can now formulate an algorithm for the computation of the kronecker (and so the Legendre) Symbol: after checking b is not zero, we can extract all the factor 2 from b and a, and then use the reciprocity law and the periodicity, until a becomes zero.

```
if $b = 0$ then
    if $|a| = 1$ then return 1
    else
        return 0
    end if
end if
if $b, a$ even then return 0
end if
$b = 2^v b'$, $b \leftarrow b'$ with $b'$ odd
if $v$ even then
    $k \leftarrow 1$
else
    $k \leftarrow (-1)^{(a^2-1)/8}$
end if
```

```
if $b < 0$ then
    $b \leftarrow -b$
    if $a < 0$ then
        $k \leftarrow -k$
    end if
end if
if $a = 0$ then
    if $b > 1$ then return $0$
    else
        return $k$
    end if
end if
$a = 2^s a'$, $a \leftarrow a'$ with $a'$ odd
if $s$ odd then
    $k \leftarrow (-1)^{(b^2-1)/8} \cdot k$
end if
$k \leftarrow (-1)^{(a-1)(b-1)/4} \cdot k$
$r \leftarrow |a|$, $a \leftarrow b \pmod{r}$, $b \leftarrow r$
Go to the check $a = 0$
```

The cycle in the algorithm repeat itself the same times as the Euclidean algorithm, that is $\log(N)$ times, with $N \geq a, b$. Through an accurate implementation of the algorithm, the cycles have a complexity of the magnitude of the logarithm, so the whole program has a complexity of $O(\log^2(N))$.

Moreover, thanks to the results above, the algorithm is correct and always terminates.

Another similar algorithm uses the fact that, if a and b are odd, then $a - b$ is even, and since we know how to handle the factors 2, we can avoid the modulus operation. The difference with the last algorithm is very little, so we write only the commands that substitute the last three lines:

```
$r \leftarrow b - a$
if $r > 0$ then
    $k \leftarrow (-1)^{(a-1)(b-1)/4} \cdot k$
    $b \leftarrow a$, $a \leftarrow r$
else
    $a \leftarrow -r$
end if
Go to the check $a = 0$
```

Lastly, we notice that the Kronecker Symbol has been introduced only to compute the Legendre Symbol, but does not really indicates if a is a quadratic residue modulus b, so we can write a simpler algorithm in order to compute only the Legendre Symbol: given p an odd prime and $0 \leq a < p$ an integer, then a lot of commands are not useful. Deleting them, we obtain

```
**if** $a = 0$ **then return** $0$
**end if**
$k \leftarrow 1$
$b \leftarrow p$
$a = 2^v a'$, $a \leftarrow a'$ with $a'$ odd
**if** $v$ odd **then** $k \leftarrow (-1)^{(p^2-1)/8} * k$
**end if**
**if** $a = 1$ **then return** $k$
**end if**
$k \leftarrow (-1)^{(a-1)(b-1)/4} \cdot k$
$r \leftarrow b \pmod{a}$, $b \leftarrow a$, $a \leftarrow r$
Go to line 5
```

Some tricks to diminish the complexity of the algorithms are the following:

- Defining $tab2[\,] = \{0, 1, 0, -1, 0, -1, 0, 1\}$, we can rewrite the line

$$k \leftarrow (-1)^{(p^2-1)/8} * k \qquad \rightleftarrows \qquad k \leftarrow tab2[p\&7] * k$$

- If a and b are odd, then $(-1)^{(a-1)(b-1)/4} = -1$ if and only if both a and b are $a \equiv b \equiv 3 \pmod{4}$. So we can rewrite the command

$$k \leftarrow (-1)^{(a-1)(b-1)/4} * k \qquad \rightleftarrows \qquad k \leftarrow (a\&b\&2) * k$$

- The operation $n/2$ is substituted by $n >> 1$.