Computer Science & Engineering Department

IIT Kharagpur

Computational Number Theory: CS60094

Lecture V

Instructor: Goutam Biswas *Spring Semester 2014-2015*

1 Basic Properties of Integers IV

1.1 Legendre Symbol

Definition 1: Let p be an odd prime and $a \in \mathbb{Z}$. We know that there is a $b \in \mathbb{Z}_p$ such that $a \equiv b(\text{mod } p)$. We define the *Legendre Symbol* $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } b = 0 \text{ i.e. } p|a, \\ 1 & \text{if } b \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } b \text{ is a quadratic non-residue modulo } p. \end{cases}$$

In fact $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Example 1. Consider the congruence $x^2 \equiv a \pmod{11}$. We know that $10^2 \equiv 1 \pmod{11}$, $5^2 \equiv 3 \pmod{11}$, $4^2 \equiv 5 \pmod{11}$, $8^2 \equiv 9 \pmod{11}$, $9^2 \equiv 4 \pmod{11}$. So $\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1$. But $\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1$. $\left(\frac{0}{11}\right) = \left(\frac{22}{11}\right) = \left(\frac{-33}{11}\right) = \cdots = 0$, $\left(\frac{18}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{-4}{11}\right) = \cdots = -1$, and $\left(\frac{15}{11}\right) = \left(\frac{4}{p}\right) = \left(\frac{-7}{11}\right) = \cdots = 1$.

Proposition 1. Let p be an odd prime and let $a, b \in \mathbb{Z}$. Following are a few properties of the Legendre symbol.

1. If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{a^2}{p}\right) = 1$.
3. $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
5. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$. Any square factor of the 'numerator', relatively prime to the 'denominator', can be removed from the Legendre symbol.
6. $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. So
$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

Proof:

1. Both $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ either have same set of solutions, or have no solutions.
2. $x^2 \equiv a^2 \pmod{p}$ has a trivial solution a.
3. If a is a quadratic residue of p, then $a^{(p-1)/2} \equiv 1 \equiv \left(\frac{a}{p}\right)(\text{ mod } \ p)$. Similarly, if a is a quadratic non-residue of p, then $a^{(p-1)/2} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}$.
4. From (3) we get $\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(\text{mod } p)$. But $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$, implies $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right)$.
5. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right) \times 1 = \left(\frac{a}{p}\right)$.
6. The first part is directly from (2) where $a = 1$. For the second part, we use (4) and substitute -1 for a.
If $p \equiv 1 \pmod{4}$, then $\frac{p-1}{2}$ is even and it is odd if $p \equiv 3 \pmod{4}$.

QED.

Example 2. We find the value of $\left(\frac{-23}{59}\right)$. We know $-23 \equiv 36 \pmod{59}$, so $\left(\frac{-23}{59}\right) = \left(\frac{36}{59}\right) = \left(\frac{6^2}{59}\right) = 1$.

We have already proved that there are infinitely many primes of the form $4k+1$. We used the fact that -1 is a quadratic residue of an odd prime if and only if it is of the form $4k+1$. The same proof can be written using the Legendre symbol as follows.

Proof: Let there be finitely many such primes, namely $p_1, p_2, \cdots, p_k$, and $n = 4m^2 + 1$, where $m = p_1 \cdots p_k$. It is clear that n is odd and there is an odd prime $p|n$. So, $4m^2 \equiv -1 \pmod{p}$. In terms of Legendre symbol we have $\left(\frac{-1}{p}\right) = 1$. So p is of the form $4k+1$. But that is impossible as p cannot be any one p_i. So there must be infinitely many primes. QED.

Proposition 2. If p is an odd prime, then

$$\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0.$$

The proof come from the basic definition and the number of quadratic residue and quadratic non-residue modulo p.

Proposition 3. If r be a *generator* of $\mathbb{Z}_p^*$ (*primitive root* of p), then even powers of r are quadratic residues modulo p, and odd powers of r are the quadratic non-residue modulo p.

Example 3. Let $p = 11$, $\mathbb{Z}_{11}^* = \{1, 2, \cdots, 10\}$. Consider the *primitive root (generator)* 2 and its powers,

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 5, 2^5 \equiv 10, 2^6 \equiv 9, 2^7 \equiv 7, 2^8 \equiv 3, 2^9 \equiv 6, 2^{10} \equiv 1 \pmod{11}.$$

Now we have

$$9^2 \equiv 4, 4^2 \equiv 5, 8^2 \equiv 9, 5^2 \equiv 3, 10^2 \equiv 1 \pmod{11}.$$

So the even powers of the primitive root 2 are quadratic residue modulo 11.

Lemma 4. (*Gauss*)
Let p be an odd prime and let a be an integer such that $gcd(a, p) = 1$. Consider the set

$$S = \{a, 2a, 3a, \cdots, \frac{p-1}{2}a\}.$$

Define $A = \{b \in S : \ b \bmod p > \lfloor p/2 \rfloor\}$, if $|A| = n$, then

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

Example 4. Let $p = 11$ and $a = 4$. $S = \{4, 8, 12, 16, 20\}$. The set of remainders are $\{4, 8, 1, 5, 9\}$. So $n = |\{8, 9\}| = 2$ and $\left(\frac{4}{11}\right) = (-1)^2 = 1$ i.e 4 is a quadratic residue of 11, $9^2 \equiv 4 \pmod{11}$.

Proof: For any $x \in S$, $x \not\equiv 0 \pmod{p}$, as $x = a\alpha$ and both a and α are relatively prime to p.

It is also the case that no two of them are congruent modulo p. Let $x, y \in S$, and $x = a\alpha$ and $y = a\beta$. But $p \not| a(\alpha - \beta)$.

So all the remainders of the elements of S modulo p are distinct and non-zero.

Let $r_1, \cdots, r_m$ be the set of remainders so that $0 < r_i \leq \frac{p-1}{2}$, and $s_1, \cdots, s_n$ be the set of remainders so that $\frac{p+1}{2} \leq s_i < p$, where $m + n = \frac{p-1}{2}$.

Consider the sequence $(p - s_1), \cdots, (p - s_n)$. Each term $p - s_i$ is greater than zero and is less than or equal to $p - \frac{p+1}{2} = \frac{p-1}{2}$. We claim that $r_1, \cdots, r_m, p - s_1, \cdots, p - s_n$ are all distinct. Otherwise, if $p - s_i = r_j$, we have $s_i + r_j = p$. But then $s_i \equiv a\alpha \pmod{p}$ and $r_j \equiv a\beta \pmod{p}$ for some α, β, $1 \leq \alpha, \beta \leq \frac{p-1}{2}$. Implies that $a(\alpha + \beta) \equiv 0 \pmod{p}$. But that is not possible as $1 < \alpha + \beta < p$.

So we have $1 \leq r_1, \cdots, r_m, (p - s_1), \cdots, (p - s_n) < \frac{p}{2}$. All of them are distinct, and they are $\frac{p-1}{2}$ in number. So their values cannot be other than $1, 2, \cdots, \frac{p-1}{2}$, and the product is $[(p-1)/2]!$. So,

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &\equiv r_1 \cdots r_m (p - s_1) \cdots (p - s_n) \\
&\equiv r_1 \cdots r_m (-s_1) \cdots (-s_n) \pmod p \\
&\equiv (-1)^n r_1 \cdots r_m s_1 \cdots s_n \pmod p \\
&\equiv (-1)^n a \cdot 2a \cdot \cdots \cdot \frac{p-1}{2} a \pmod p \\
&\equiv (-1)^n a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod p \\
1 &\equiv (-1)^n a^{\frac{p-1}{2}} \pmod p \\
a^{\frac{p-1}{2}} &\equiv (-1)^n \pmod p
\end{aligned}$$

Two points to note: (i) each remainder is congruent modulo p to exactly one element of S, so the 3rd to 4th step, and (ii) $\left(\frac{p-1}{2}\right)!$ is relatively prime to p, so the cancellation.

From Legendre symbol and Euler's criterion we know that $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\bmod\ p)$, so $\left(\frac{a}{p}\right) = (-1)^n$. QED.

Example 5. Let p be an odd prime and let a be an integer such that $gcd(a, p) = 1$. Consider the set

$$S = \left\{ \frac{p+1}{2} a, \frac{p+3}{2} a, \cdots, (p-1)a \right\}.$$

Define $A = \{b \in S : \ b \bmod p < p/2\}$, if $|A| = m$, then

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

Proposition 5. If p is an odd prime and a is an integer such that $gcd(a, p) = 1$, then

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor ka/p \rfloor}, \text{ if } a \text{ is odd},$$

and

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

Proof: Let us consider the set

$$S = \left\{ a, 2a, \cdots, \frac{p-1}{2} a \right\}.$$

We can express each element of S as

$$ak = pq_k + t_k, \ 0 < t_k < p,$$

where $1 \leq k \leq \frac{p-1}{2}$. The value of t_k cannot be zero as $p \not| ak$. Clearly $q_k = \left\lfloor \frac{ak}{p} \right\rfloor$ and we can write

$$ak = \left\lfloor \frac{ak}{p} \right\rfloor p + t_k,$$

for all k, $1 \leq k \leq \frac{p-1}{2}$.

Similar to the proof of Gauss' theorem, we divide the set of remainders in two groups, $1 \leq r_1, r_2, \cdots, r_m \leq \frac{p-1}{2}$ and $\frac{p+1}{2} \leq s_1, s_2, \cdots, s_n < p$, where $m + n = \frac{p-1}{2}$. So we have,

$$\sum_{k=1}^{\frac{p-1}{2}} ak = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor p + \sum_{k=1}^{\frac{p-1}{2}} t_k = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor p + \sum_{i=1}^{m} r_i + \sum_{i=1}^{n} s_i. \tag{1}$$

We already know that $r_1, r_2, \cdots, r_m, p-s_1, p-s_2, \cdots, p-s_n$ is a permutation of $1, 2, \cdots, \frac{p-1}{2}$. So,

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{m} r_i + \sum_{i=1}^{n} (p - s_i) = pn + \sum_{i=1}^{m} r_i - \sum_{i=1}^{n} s_i. \tag{2}$$

Subtracting (2) from (1), we get,

$$(a-1) \sum_{k=1}^{\frac{p-1}{2}} k = p \left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor - n \right) + 2 \sum_{i=1}^{m} s_i. \tag{3}$$

But we know that $\sum_{k=1}^{\frac{p-1}{2}} k = \frac{p^2-1}{8}$. So we get

$$(a-1) \cdot \frac{p^2-1}{8} \equiv \left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor - n \right) \pmod 2, \tag{4}$$

$p \equiv 1(\text{mod } 2)$.

If a is odd, then $a \equiv 1(\text{mod } 2)$ and we have

$$n \equiv \left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor \right) \pmod 2. \tag{5}$$

From the Gausses theorem we have

$$\left(\frac{a}{p} \right) = (-1)^n = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ak}{p} \rfloor}.$$

If $a = 2$, then

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{2k}{p} \right\rfloor = 0,$$

as each numerator is less than p. So

$$n \equiv \frac{p^2-1}{8} (\text{mod } 2),$$

$n \equiv -n(\text{mod } 2)$. Again using Gauss' theorem we get

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

QED.

We observe that $\frac{p^2-1}{8}$ is even if $p \equiv \pm 1(\text{ mod } 8)$ and it is odd if $p \equiv \pm 3(\text{ mod } 8)$. So we have the following conclusion.

$$\left(\frac{2}{p} \right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8, \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8. \end{cases}$$

Proposition 6. There are infinitely many primes of the form $8k - 1$ i.e. $8l + 7$.
Proof: Let there be finite number of such primes, $p_1, p_2, \cdots, p_k$. Define

$$n = (4m)^2 - 2, \; m = \prod_{i=1}^{k} p_k.$$

n is of the form $2(8(m^2 - 1) + 7)$. Let p be an odd prime divides n. We have

$$(4p_1p_2 \cdots p_k)^2 \equiv 2 \pmod p,$$

i.e. 2 is a *quadratic residue* modulo p, implies that, $\left(\frac{2}{p}\right) = 1$. Using the previous proposition we get $p \equiv \pm 1 \pmod 8$. If all odd prime divisors of n are of the form $8k+1$, then n must be of the same form. But n is of the form $2(8k+7)$ which is impossible. So it must have a divisor of the form $8l+7$. But this p cannot be equal to any of the p_i's. So there is a contradiction. QED.

Example 6. Let $p = 11$ and $a = 5$. $S = \{5, 10, 15, 20, 25\}$. So,

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor = 0 + 0 + 1 + 1 + 2 = 4.$$

So, $\left(\frac{5}{11}\right) = (-1)^4 = 1$ i.e. 5 is a quadratic residue of 11.

1.2 Quadratic Reciprocity Law

Let p and q be distinct odd primes. The question is whether the the following pair of quadratic congruence are solvable.

$$x^2 \equiv p \pmod q, \; y^2 \equiv q \pmod p. \tag{6}$$

Using Legendre's symbol the question is how $\left(\frac{p}{q}\right)$ is related to $\left(\frac{q}{p}\right)$. Following is a small portion of the infinite table of $\left(\frac{p}{q}\right)$.

	p						
$q \downarrow$	3	5	7	11	13	17	19
3	0	$-$	$+$	$-$	$+$	$-$	$+$
5	$-$	0	$-$	$+$	$-$	$-$	$+$
7	$-$	$-$	0	$+$	$-$	$-$	$-$
11	$+$	$+$	$-$	0	$-$	$-$	$-$
13	$+$	$-$	$-$	$-$	0	$+$	$-$
17	$-$	$-$	$-$	$-$	$+$	0	$+$
19	$-$	$+$	$+$	$+$	$-$	$+$	0

From the very small portion of the table we observe that *row-5* and *column-5* are identical. Similar is the case for *row-13*, *column-13*, and *row-17*, *column-17.* There is slightly more complicated regularity in cases of 3, 7, 11, and 19. There is a flip in sign when both $p, q \equiv 3(\bmod 4)$. If one of p or q is of the form $4k+1$, then it seems that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$, and if both are of the form $4k+3$, then it seems that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$. If

The relation was guessed by Euler and an incomplete proof was given by Legendre. Gauss rediscovered it at the age of 18 and obtained the first complete proof. In fact he gave several proofs. It is well known as *Quadratic Reciprocity Law*,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

The law states that if one of p or q has remainder 1 when divided by 4, then either both are solvable or both are unsolvable. If the remainders of both p and q are 3, then if one is solvable then the other is not.

Theorem 7. (*Quadratic Reciprocity Law* - Euler, Legendre, Gauss) If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Note: If $p \equiv 1(\bmod 4)$ or $q \equiv 1(\bmod 4)$, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$ i.e. either $\left(\frac{p}{q}\right) = 1 = \left(\frac{q}{p}\right)$ or $\left(\frac{p}{q}\right) = -1 = \left(\frac{q}{p}\right)$ i.e. either p is a *quadratic residue* modulo q and q is a *quadratic residue* modulo p, or p is a *quadratic non-residue* modulo q and q is a *quadratic non-residue* modulo p.

If both $p \equiv -1(\bmod 4)$ and $q \equiv -1(\bmod 4)$, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$ i.e. either $\left(\frac{p}{q}\right) = -1$ or $\left(\frac{q}{p}\right) = -1$, but not both i.e. p is a *quadratic residue* modulo q if and only if q is a *quadratic non-residue* modulo p. Following example clearly explains it.

Example 7.

1. $p = 13 = 4 \cdot 3 + 1$ and $q = 3 = 4 \cdot 0 + 3$: We observe that $4^2 \equiv 3 (\text{mod } 13)$ and $1^2 \equiv 13(\text{mod } 3)$.
2. $p = 13 = 4 \cdot 3 + 1$ and $q = 7 = 4 \cdot 1 + 3$: We observe that 7 is not a perfect square modulo 13. Also 13 is not a perfect square modulo 7.
3. $p = 19 = 4 \cdot 4 + 3$ and $q = 7 = 4 \cdot 1 + 3$: We observe that $19 \equiv 5(\text{mod } 7)$ and 5 is not a perfect square modulo 7. But $8^2 \equiv 7(\text{mod } 19)$ i.e. 7 is a perfect square modulo 19.

Proof: Ferdinand Eisenstine's proof
We consider a rectangle of vertex co-ordinates, $(0, 0)$, $(p/2, 0)$, $(0, q/2)$, and $(p/2, q/2)$. Let R be the internal region of the rectangle (excluding the perimeter points). We count the number of *lattice points* (points with integer coordinates) of R in two different ways.
It is the collection of all the points whose co-ordinates are (x, y) so that $1 \leq x \leq \frac{p-1}{2}$ and $1 \leq y \leq \frac{q-1}{2}$. So number of such points are,

$$\frac{p-1}{2} \times \frac{q-1}{2}.$$

Consider the diagonal joining $(0, 0)$ and $(p/2, q/2)$. Its equation is $y = mx$, where $m = \frac{q}{p}$ i.e. $py = qx$. We claim that there is no lattice point on the diagonal within R. If a lattice point (u, v) is on the diagonal within R, then $pv = qu$, implies that $q|pv$. But $gcd(p, q) = 1$ and $0 < v < q$ - so it is impossible.
Let R_a and R_b be the regions of R above and below the diagonal. Number of lattice points within R are the number of lattice points of R_a and R_b.
We know that the number of integers in the interval $(0, \frac{kq}{p})$ are $\lfloor \frac{kq}{p} \rfloor$. So for each k, $1 \leq k \leq \frac{p-1}{2}$, there are $\lfloor \frac{kq}{p} \rfloor$ lattice points above $(k, 0)$ in R_b. So the total number of lattice points in R_b are

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor.$$

By a similar calculation, number of lattice points in R_a are

$$\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

So we have

$$\frac{p-1}{2} \times \frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor$$

But we know that

$$\begin{aligned} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\sum_{k=1}^{\frac{q-1}{2}} \lfloor \frac{kp}{q} \rfloor} \cdot (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor} \\ &= (-1)^{\sum_{k=1}^{\frac{q-1}{2}} \lfloor \frac{kp}{q} \rfloor + \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \end{aligned}$$

QED.

Corollary 8. If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ (mod 4) or } q \equiv 1 \text{ (mod 4)}, \\ -1 & \text{if } p \equiv 3 \text{ (mod 4) and } q \equiv 3 \text{ (mod 4)}. \end{cases}$$

In other words,

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \text{ (mod 4) or } q \equiv 1 \text{ (mod 4)}, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \text{ (mod 4) and if } q \equiv 3 \text{ (mod 4)}. \end{cases}$$

Proof: $\frac{p-1}{2}\frac{q-1}{2}$ is even if and only if one of the primes is of the form $4k+1$. The product is odd if both are of the form $4k+3$. QED.

Example 8. Evaluate the Legendre symbol $\left(\frac{-219}{383}\right)$.
We have $\left(\frac{-219}{383}\right) = \left(\frac{(-1\times3\times73)}{383}\right) = \left(\frac{-1}{383}\right)\left(\frac{3}{383}\right)\left(\frac{73}{383}\right) = -\left(\frac{3}{383}\right)\left(\frac{73}{383}\right)$, as $383 \equiv 3 \pmod 4$.
$\left(\frac{3}{383}\right) = -\left(\frac{383}{3}\right) = -\left(\frac{2}{3}\right) = -1\times -1 = 1$, as $383 \equiv 2 \pmod 3$.
$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right)$ as $73 \equiv 1 \pmod 4$.
$\left(\frac{383}{73}\right) = \left(\frac{18}{73}\right)$ as $383 \equiv 18 \pmod{73}$.
$\left(\frac{18}{73}\right) = \left(\frac{(2\times3^2)}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{3^2}{73}\right) = 1\times1 = 1$, as $73 \equiv 1 \ (\bmod\ 8)$. So $\left(\frac{-219}{383}\right) -1\times1\times1 = -1$.

Let q be an odd prime > 3. Let $p = 3$ so we have $p = 3 \equiv 3 \pmod 4$. We already know

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

So

$$\left(\frac{3}{q}\right) = \begin{cases} \left(\frac{q}{3}\right) & \text{if } q \equiv 1 \pmod 4, \\ -\left(\frac{q}{3}\right) & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

So $q \equiv \pm1 \pmod 3$. If $q \equiv 1 \pmod 3$, then $\left(\frac{q}{3}\right) = \left(\frac{1}{3}\right) = 1$. If $q \equiv -1 \pmod 3$, then $\left(\frac{q}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$ i.e.

$$\left(\frac{q}{3}\right) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 3, \\ -1 & \text{if } q \equiv -1 \pmod 3. \end{cases}$$

So the value of $\left(\frac{3}{q}\right) = 1$ if and only if [$q \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 3$] or [$q \equiv 3 \pmod 4$ and $q \equiv 2 \pmod 3$]. This is equivalent to, $\left(\frac{3}{q}\right) = 1$ if and only if $q \equiv \pm1 \pmod{12}$. So we have the following theorem.
Proposition 9. If p is an odd prime > 3, then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm5 \pmod{12}. \end{cases}$$

1.3 Jacobi Symbol

Jacobi symbol is a generalisation of Legendre's symbol as follows:
Definition 2: Let n be an odd positive integer so that $n = p_1p_2\cdots p_k$, where $p_1, p_2, \cdots, p_k$ are odd primes (need not be distinct), and let a be any integer, then we define

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{if } gcd(a,n) > 1, \\ \prod_{i=1}^{k} \left(\frac{a}{p_i}\right) & \text{otherwise.} \end{cases}$$

where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol. For completion $\left(\frac{a}{1}\right) = 1$ by definition.

Example 9.

$$\left(\frac{21}{275}\right) = \left(\frac{21}{5}\right)^2\left(\frac{21}{11}\right) = \left(\frac{7}{5}\right)^2\left(\frac{3}{5}\right)^2\left(\frac{7}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{2}{5}\right)^2\left(\frac{3}{5}\right)^2 \times(-1)\times1 = -1.$$

The correspondence of quadratic residue with Legendre symbol is one-to-one. But that is not true for Jacobi symbol.

Example 10. $\left(\frac{8}{15}\right) = \left(\frac{8}{3}\right)\left(\frac{8}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{5}\right) = (-1)\cdot(-1) = 1$, but there is no solution of $x^2 \equiv 8 (\bmod\ 15)$.

Following are a few properties of Jacobi Symbol.
Proposition 10. Let m, n be odd positive integers and a, b are integers, then we have

1. $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$,

2. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$,

3. $a \equiv b \pmod{m} \Rightarrow \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$. In other words, $\left(\frac{a+km}{m}\right) = \left(\frac{a}{m}\right)$.

4. $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$,

5. $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$,

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

Proof: Let $m = p_1p_2\cdots p_k$ and $n = q_1q_2\cdots q_l$ where p_i's and q_i's are primes; they need not be distinct.

1. $\left(\frac{ab}{m}\right) = \prod_{i=1}^{k}\left(\frac{ab}{p_i}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)\prod_{i=1}^{k}\left(\frac{b}{p_i}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.

2. $\left(\frac{a}{mn}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)\prod_{i=1}^{l}\left(\frac{a}{q_i}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

3. $a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{p_i}$, for all $i = 1, \cdots, k$. So, $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$, for all $i = 1, \cdots, k$. Finally, $\left(\frac{a}{m}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right) = \prod_{i=1}^{k}\left(\frac{b}{p_i}\right) = \left(\frac{b}{m}\right)$.

4. We know that for odd integer $n_1, n_2, \cdots, n_k$,

$$\sum_{i=1}^{k}\frac{n_i-1}{2} \equiv \frac{\prod_{i=1}^{k} n_i - 1}{2} \pmod{2}.$$

So we have

$$\begin{aligned}
\left(\frac{-1}{m}\right) &= \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_k}\right)\\
&= (-1)^{\frac{p_1-1}{2}}\cdot(-1)^{\frac{p_2-1}{2}}\cdot\cdots\cdot(-1)^{\frac{p_k-1}{2}}\\
&= (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_k-1}{2}}\\
&= (-1)^{\frac{p_1p_2\cdot\cdots\cdot p_k-1}{2}} = (-1)^{\frac{m-1}{2}}.
\end{aligned}$$

5. We know that for odd integer $n_1, n_2, \cdots, n_k$,

$$\sum_{i=1}^{k}\frac{n_i^2-1}{8} \equiv \frac{\prod_{i=1}^{k} n_i^2 - 1}{8} \pmod{2}.$$

So we have

$$\begin{aligned}
\left(\frac{2}{m}\right) &= \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_k}\right)\\
&= (-1)^{\frac{p_1^2-1}{8}}\cdot(-1)^{\frac{p_2^2-1}{8}}\cdot\cdots\cdot(-1)^{\frac{p_k^2-1}{8}}\\
&= (-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_k^2-1}{8}}\\
&= (-1)^{\frac{p_1^2p_2^2\cdot\cdots\cdot p_k^2-1}{2}} = (-1)^{\frac{m^2-1}{2}}.
\end{aligned}$$

6.

$$\begin{aligned}
\left(\frac{n}{m}\right) &= \left(\frac{q_1q_2\cdots q_l}{p_1p_2\cdots p_k}\right),\\
&= \left(\frac{q_1q_2\cdots q_l}{p_1}\right)\cdots\left(\frac{q_1q_2\cdots q_l}{p_k}\right),\\
&= \left(\frac{q_1}{p_1}\right)\cdots\left(\frac{q_l}{p_1}\right)\cdots\left(\frac{q_1}{p_k}\right)\cdots\left(\frac{q_l}{p_k}\right),\\
&= (-1)^{\frac{q_1-1}{2}\frac{p_1-1}{2}}\left(\frac{p_1}{q_1}\right)\cdots(-1)^{\frac{q_l-1}{2}\frac{p_1-1}{2}}\left(\frac{p_1}{q_l}\right)\cdots(-1)^{\frac{q_1-1}{2}\frac{p_k-1}{2}}\left(\frac{p_k}{q_1}\right)\cdots(-1)^{\frac{q_l-1}{2}\frac{p_k-1}{2}}\left(\frac{p_k}{q_l}\right),\\
&= (-1)^{\frac{q_1-1}{2}\frac{p_1-1}{2}+\cdots+\frac{q_l-1}{2}\frac{p_1-1}{2}+\cdots+\frac{q_1-1}{2}\frac{p_k-1}{2}+\cdots+\frac{q_l-1}{2}\frac{p_k-1}{2}}\left(\frac{m}{n}\right),\\
&= (-1)^{(\frac{q_1-1}{2}+\cdots+\frac{q_l-1}{2})(\frac{p_1-1}{2}+\cdots+\frac{p_k-1}{2})}\left(\frac{m}{n}\right),\\
&= (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{m}{n}\right).
\end{aligned}$$

QED.

This theorem is very important from the computational point of view. Note that

- $(-1)^{\frac{n-1}{2}} = 1$ if and only if $n \equiv 1 \pmod 4$,
- $(-1)^{\frac{n^2-1}{8}} = 1$ if and only if $n \equiv \pm 1 \pmod 8$,
- $(-1)^{\frac{m-1}{2}\frac{n-1}{2}} = 1$ if and only if $n \equiv 1 \pmod 4$ or $m \equiv 1 \pmod 4$.

What is the interpretation of the Jacobi Symbol?
If a is a quadratic residue modulo n, an odd integer, then there is some $b \in \mathbb{Z}_n^*$ so that $b^2 \equiv a \pmod n$, and $gcd(a, n) = 1$. So we have $\left(\frac{a}{n}\right) = \left(\frac{b^2}{n}\right) = \left(\frac{b}{n}\right)^2 = 1$. But it is not the case that $\left(\frac{a}{n}\right) = 1$ implies that a is a quadratic residue of n.

Example 11. We know that $\left(\frac{2}{3}\right) = -1 = \left(\frac{2}{5}\right)$ i.e. 2 is quadratic non-residue of both 3 and 5. But $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = -1 \times -1 = 1$. But 2 cannot be a quadratic residue of 15 as it is not so for its prime factors.

1.4 Computation of Jacobi Symbol

All these laws can be used to design efficient procedure to compute Jacobi symbol.

Let a be an arbitrary integer and $n \geq 3$ be an odd integer. We like to compute $\left(\frac{a}{n}\right)$.

1. If $a \notin \mathbb{Z}_n$, then compute $\left(\frac{a \bmod n}{n}\right)$.
2. If $a = 0$, then the value is 0.
3. If $a = 1$, then the value is 1.
4. If $4|a$, then compute $\left(\frac{a/4}{n}\right)$. The reason is $\left(\frac{2^2 b}{n}\right) = \left(\frac{2}{n}\right)^2\left(\frac{b}{n}\right) = \left(\frac{b}{n}\right)$.
5. If $2|a$, then if $n \equiv \pm 1 (\bmod 8)$, then compute $\left(\frac{a/2}{n}\right)$, else compute $-\left(\frac{a/2}{n}\right)$. The reason is $\left(\frac{2b}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{b}{n}\right)$, if $n \equiv \pm 1 (\bmod 8)$, otherwise $= -\left(\frac{b}{n}\right)$
6. If ($a > 1$ and $a \equiv 1 \pmod 4$) or $n \equiv 1 \pmod 4$, then compute $\left(\frac{n \bmod a}{a}\right)$.
7. If $a \equiv 3 \pmod 4$ and $n \equiv 3 \pmod 4$, then compute $-\left(\frac{n \bmod a}{a}\right)$.

Following procedure computes Jacobi symbol.

```
$jacobi(a, n)$ // n is odd $\geq 3$
1   $num \leftarrow a \bmod n$
2   $den \leftarrow n$
3   $sign \leftarrow 1$
4   while $(num \geq 2)$
5       while $(4 \mid num)$, $num \leftarrow num / 4$
6       if $(2 \mid num)$ then
7           if $(den \bmod 8) \in \{3, 5\}$ then $sign \leftarrow (-\, sign)$
8           $num \leftarrow num / 2$
9       if $(num = 1)$ then break
10      if $(num \bmod 4) = 3 = (den \bmod 4)$ then $sign \leftarrow (-\, sign)$
11      $(num, den) \leftarrow (den \bmod num, num)$
12  return $sign \times num$
```

The values of $a \bmod n$, and n are stored in the variables num and den respectively. At the beginning, $num < den$. The loop of 4-11 is executed as long as num is not equal to 0 or 1. The value of $sign \times num$ is returned at the end of the loop, where the variable `sign` holds a value from $\{1, -1\}$. The value of $sign$ changes at 7 and 10. In line-7, if $num = 2k$ and $den \bmod 8 \in \{3, 5\}$, then $\left(\frac{num}{den}\right) = \left(\frac{2k}{den}\right) = \left(\frac{2}{den}\right)\left(\frac{k}{den}\right) = -\left(\frac{k}{den}\right)$. Similarly, the sign change in line-10 is due to the *quadratic reciprocity law*.

If the value of $gcd(a, n) > 1$, the value of num will be 0 at some stage, while $den \geq 3$. It is not necessary to compute $gcd(a, n)$ explicitly. Note that the *gcd(num, den)* $= gcd(a, n)$. *den* is an odd number, so the division of *num* by 2 or 4 does not change the value of the *gcd*.

The value of *num* at line-10 is odd, it is less than *den*, and greater than 1. At line-11 we compute $\left(\frac{den \bmod num}{num}\right)$. Sign is adjusted properly at line-10.

Following the analysis of Euclid's algorithm, the line 4-11 loop cannot be executed more than $O(\log n)$ times. This is a outcome of quadratic reciprocity law.

Proposition 11. The algorithm *jacobi()* returns the value $\left(\frac{a}{n}\right)$. The number of iterations of the loop is $O(\log n)$.

Proof: We claim that after line (3),

$$\texttt{sign} \cdot \left(\frac{num}{den}\right) = \left(\frac{a}{n}\right).$$

It is true for line (5), (6-8), (10-11) following our discussion.

The analysis of the number of iteration of the loop is similar to that of the *gcd-algorithm*. Let the sequence of values at (4) be

$$(num_0, den_0), (num_1, den_1), \cdots, (num_t, den_t), \cdot.$$

The value of $c_0 = n$ and $c_{t+2} \leq \frac{c_t}{2}$. So the number of iterations cannot be more than $2 \log n$. QED.

References

[AD] *Computational Number Theory* by Abhijit Das, Pub. CRC Press, 2013, ISBN 978-1-4398-6615-3.

[MD] *Primality Testing in Polynomial Time From Randomized Algorithms to "PRIMES is in P"*, by Martin Dietzfelbinger, LNCS 3000 (Tutorial), Pub. Springer, 2004, ISBN 3540403442.

[VS] *A Computational Introduction to Number Theory and Algebra* by Victor Shoup, 2nd ed., Pub. Cambridge University Press, 2009, ISBN 978-0-521-51644-0.

[EBV] *A Course in Algebra* by E B Vinberg, Graduate Studies in Mathematics, vol. 56, Pub. American Mathematical Society (Universities Press 2009), ISBN 978-0-8218-4858-6.