Quadratic Reciprocity Law

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500 046
kumaresa@gmail.com

Abstract

This set of notes is written for the benefit of teachers and participants of MTTS Programme. We assume that the readers have gone though a one-semester course of algebra and are reasonably comfortable with groups, rings and fields.

Definition 1. Let $p \in \mathbb{N}$ be a prime. We say that $a \in \mathbb{Z}$ is a square modulo the prime p if there exists an integer $b \in \mathbb{Z}$ such that $b^2 \equiv a \pmod{p}$. Observe that this is equivalent saying that the polynomial $X^2 - a \in \mathbb{Z}_p[X]$ has a root in the field $\mathbb{Z}_p$. (Here, as is customary, a stands for the congruence class $[a] \in \mathbb{Z}_p$.) In classical number theory texts, one also says that a is a quadratic residue modulo p, as $b^2 \equiv a \pmod{p}$ holds. If a is not a quadratic residue modulo p, then a is called a quadratic non-residue modulo p.

Why should one be interested in this concept? After solving linear congruences $ax \equiv b \pmod{m}$, one is tempted to solve quadratic congruences of the form $ax^2 + bx + c \equiv 0 \pmod{m}$. When one employs the completing the square trick, one is faced with problems of the kind $ax^2 \equiv b \pmod{m}$. Also, in classical number theory one is also interested in finding/characterizing the primes which are represented by quadratic forms over $\mathbb{Z}$. In this context also, one is led to problems of the type above.

Example 2. Let $p = 7$. Since $1^2, 2^2, \ldots, 6^2$ are congruent to one of the $1, 4, 2$, we see that $1, 2, 4$ are squares modulo 7 while 3,5,6 are not.

Definition 3. A very useful device when dealing with squares modulo a prime is the Legendre symbol. Let p be a prime, $a \neq 0 \in \mathbb{Z}_p$. Then

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a square modulo } p, \\ -1, & \text{if } a \text{ is not a square modulo } p. \end{cases}$$

Remark 4. The subset S of squares in $G := \mathbb{Z}_p^*$ is indeed a subgroup of index 2. If g is a generator of G, then $S = \{g^2, g^4, \ldots, g^{\frac{p-1}{2}2} = 1\}$. If we identify G/H with the multiplicative group $\{\pm 1\}$, then $\psi \colon G \to G/H \simeq \{\pm]$ defined by $\psi(a) := \frac{a}{p}$ is a group homomorphism.

The following result is of both theoretical and practical use.

Lemma 5 (Euler's Criterion)**.** *Let p be an odd prime. Then, for any a with* $\gcd(a,p)=1$*, we have*

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

In particular, a is a square modulo p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Proof. Let a be such that $\left(\frac{a}{p}\right)=1$. Then a is a square modulo p. Hence there exists $b \in \mathbb{Z}$ such that $b^2 \equiv a \pmod{p}$. We raise both sides of the congruence to the power $(p-1)/2$ to obtain

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 (\mathrm{mod}\, p),$$

since the order of the group $\mathbb{Z}_p^*$ is $p-1$. Hence if $\left(\frac{a}{p}\right)=1$, then we have $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Assume that $a \in \mathbb{Z}_p$ is not a square. If g is generator of the cyclic group $\mathbb{Z}_p^*$, then $a=g^r$ where $r=2k+1$. Hence

$$a^{\frac{p-1}{2}} = (g^{(2k+1)})^{\frac{p-1}{2}} = g^{k(p-1)} g^{\frac{p-1}{2}}.$$

If $(g^{\frac{p-1}{2}})^2 = g^{p-1} = 1$. Hence the order of $g^{\frac{p-1}{2}}$ is of order 2. But -1 is the only element of order 2 in $\mathbb{Z}_p^*$. (If $1 \le t \le p-1$ and if $t^2 \equiv 1 \pmod{p}$, then $p|(t+1)(t-1)$. This implies $t+1=p$ or $t=p-1=-1$ modulo p.) □

Remark 6. We can rephrase the proof in a different way. Let $\varphi(a) := a^{\frac{p-1}{2}}$. Then φ is a group homomorphism. Let $\psi(a) := \frac{a}{p}$ be the Legendre map. We claim that $\ker\psi \subset \ker\varphi$. For, if $a \in \ker\psi$, then there exists $b \in \mathbb{Z}_p^*$ such that $a=b^2$. Hence we have

$$\varphi(a) = a^{\frac{p-1}{2}} = b^{p-1} = 1.$$

Hence $\ker\psi \le \ker\varphi$. Since $\ker\psi$ is of index 2 in $\mathbb{Z}_p^*$, either $\ker\varphi = \ker\psi$ or $\ker\varphi = \mathbb{Z}_p^*$. The latter cannot happen. For, otherwise, we have $a^{\frac{p-1}{2}} = 1$ for all $a \in \mathbb{Z}_p^*$ and hence the polynomial $X^{\frac{p-1}{2}} - 1$ has $p-1$ zeros in the integral domain $\mathbb{Z}_p$, a contradiction. Hence we conclude that $\ker\varphi = \ker\psi$. That is, for all a
not $\equiv 0 (\mathrm{mod}\, p)$, we have $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

It follows from the argument above that the equation $x^2 \equiv a \pmod{p}$ has no solution iff $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Hence we arrive at the Euler's criterion $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ for all a nonzero modulo p.

Example 7. We shall do a concrete example to illustrate the power of Euler's criterion. Is $a=7$ a square modulo 37? We have $a^2 \equiv 12 \pmod{37}$, $a^4 \equiv 144 \equiv 33 \equiv -4 (\mathrm{mod}\, 37)$, $a^8 \equiv 16 (\mathrm{mod}\, 37)$, $a^{16} \equiv 256 \equiv -3 (\mathrm{mod}\, 37)$. Hence finally, we arrive at

$$a^{18} \equiv a^2 \times a^{16} \equiv 12 \times (-3) \equiv -36 \equiv 1 (\mathrm{mod}\, 37).$$

Therefore, 7 is a square modulo 37. As an exercise, check whether 11 is a square modulo 37.

Let p be any odd prime. Then exactly one of $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$ holds. If p and q are distinct odd primes, then there are two possibilities. (i) Both are congruent to 3 modulo 4 or (ii) at least one of them is congruent to 1 modulo 4.

Let $p > 2$ and $q > 2$ be two distinct primes. The law of quadratic reciprocity asserts a reciprocal relationship between the problems of existence of solutions of

$$x^2 \equiv q \pmod p \quad \text{and} \quad x^2 \equiv p \pmod q.$$

Law of Quadratic Reciprocity:
Case 1. If $p \equiv q \equiv 3 (\mathrm{mod}\, 4)$, then $x^2 \equiv q \pmod p$ has a solution iff $x^2 \equiv p \pmod q$ has no solutions, that is, $\left(\frac{q}{p}\right) = 1$ iff $\left(\frac{p}{q}\right) = -1$.
Case 2. If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$ holds, then $x^2 \equiv q \pmod p$ has a solution iff $x^2 \equiv p \pmod q$ has a solution, that is, $\left(\frac{q}{p}\right) = 1$ iff $\left(\frac{p}{q}\right) = 1$.

We need Wilson's theorem and Chinese Remainder Theorem while proving the law of quadratic law of reciprocity. Let us recall both of them.

Theorem 8 (Wilson)**.** *For any prime p, we have*

$$(p-1)! \equiv -1 \pmod p. \tag{2}$$

We also have

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p-1}{2}} (p-1)! \pmod p. \tag{3}$$

Proof. First observe that in a finite abelian group G, the product $P := \prod_{g \in G} g = \prod_{o(g)=2} g$. Now, in $G := \mathbb{Z}_p^*$ the only element of order 2 is $-1 = p-1$, as shown in the proof of Lemma 5. Thus we established (2).

We rewrite

$$(p-1)! \equiv 1(p-1) \times 2(p-2) \times \cdots \times (\frac{p-1}{2})(p - \frac{p-1}{2}) \equiv -1 \pmod p.$$

Since $p - r \equiv -r \pmod p$, we see that the displayed congruence yields

$$1(-1) \times 2(-2) \times \cdots \times (\frac{p-1}{2})(-\frac{p-1}{2}) \equiv -1 \pmod p.$$

Wilson's formula (3) follows now. □

Theorem 9 (Chinese Remainder Theorem)**.** *Let $m, n \in \mathbb{N}$ be relatively prime. Then the map $f \colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ defined by $f(k) := (k, k)$ is an isomorphism of rings. In particular, the restriction of f to $\mathbb{Z}_{mn}^*$ maps it isomorphically onto $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$.* □

The law of quadratic reciprocity is succinctly captured in the following formulation.

Theorem 10 (Law of Quadratic Reciprocity)**.** *Let $p > 2$ and $q > 2$ be two distinct primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{4}$$

Proof. Consider the (normal) subgroup $H := \{\pm(1,1)\} \leq Z_{mn}^* =: G$. Suppose that we wish to find the product of all elements of the quotient group G/H. One way of doing this would be to choose a set of coset representatives of G/H and compute their products which will be unique modulo H. If we find two different sets of coset representatives and find their product, they will differ by an element of H. The quadratic reciprocity law (4) drops out from these computations.

As the first set, let us consider $A := \{(i,j) : 1 \leq i \leq p-1, 1 \leq j \leq (q-1)/2\}$. It is easy to verify that this is a system of representatives of the cosets of H in G. (There is a symmetrically defined set A', which will also work!)

Let $B := \{(k,k) : 1 \leq k \leq (pq-1)/2;\ \gcd(k,pq) = 1\}$. Using CRT, it is again easy to verify that this is a system of representatives of the cosets of H in G.

Let $\alpha := \prod_{(i,j)\in A}$ and $\beta := \prod_{(k,k)\in B}(k,k)$.

We now compute α:

$$\begin{aligned}\prod_A (i,j) &= \left((p-1)!^{\frac{q-1}{2}}, (q-1)/2)!^{p-1}\right) \\ &= \left((p-1)!^{\frac{q-1}{2}}, (q-1)!^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right), \quad \text{using (3).} \end{aligned} \tag{5}$$

In computing β, the product of the first components, say, β_1 is taken modulo p while that (say, β_2) of the second components is taken modulo q. Since k is required to satisfy $\gcd(k,pq) = 1$, while computing β_1, we may exclude all multiples of p and then divide it by the product of multiples of q:

$$\begin{aligned}\beta_1 &= \frac{\left(\prod_{i=1}^{p-1} i\right)\left(\prod_{i=1}^{p-1} p+i\right)\cdots\left(\prod_{i=1}^{p-1}(\frac{q-1}{2}-1)p+i\right)\left(\prod_{i=1}^{\frac{p-1}{2}} \frac{q-1}{2}\cdot p+i\right)}{(1\cdot q)(2\cdot q)\cdots(\frac{p-1}{2}\cdot q)} \\ &= \frac{(p-1)!^{\frac{q-1}{2}}(\frac{p-1}{2})!}{q^{\frac{p-1}{2}}(\frac{p-1}{2})!} \\ &= \frac{(p-1)!^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} \\ &= (p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right), \quad \text{using (1)}\end{aligned}$$

Similarly, we obtain $\beta_2 = (q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$. Hence we find

$$\beta = \left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right). \tag{6}$$

Equating (5) and (6), we get

$$\left((p-1)!^{\frac{q-1}{2}}, (q-1)!^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right)H = \left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right)H. \tag{7}$$

Hence there exist $\varepsilon \in \{\pm(1,1)\}$ such that

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

That is, $\varepsilon\left(\frac{q}{p}\right) = 1$ and $\varepsilon\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Multiplying these equations yields the law. □

Remark 11. The proof of Theorem 10 follows Rosseau [1].

If you are seriously interested in number theory, you should also learn about Gauss sums and Eisenstein's proof of the law and modern ways of looking at them. A good reference for these is [2].

We give some examples illustrating QRL. We need the following properties of the Legendre symbol.

Proposition 12. *Let p be an odd prime. Let $ab \not\equiv 0 (\mathrm{mod}\, p)$. Then we have*

(i) *If $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) + \left(\frac{b}{p}\right)$.*

(ii) *We have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

(iii) $\left(\frac{a^2}{p}\right) = 1$.

Proof. (ii) follows from Euler's criterion. We have

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

□

Example 13. Compute $\left(\frac{15}{89}\right)$. Note that $15 \equiv 3 \pmod 4$ and $89 \equiv 1 \pmod 4$. hence by QRL, we have $\left(\frac{15}{89}\right) = \left(\frac{89}{15}\right)$. Since the Legendre symbol is multiplicative, we have $\left(\frac{15}{89}\right) = \left(\frac{3}{89}\right)\cdot\left(\frac{5}{89}\right)$. But $\left(\frac{3}{89}\right) = \left(\frac{89}{3}\right) = \left(\frac{2}{3}\right) = -1$. (Why?) Similarly, $\left(\frac{5}{89}\right) = \left(\frac{89}{5}\right) = \left(\frac{4}{5}\right) = 1$. Hence $\left(\frac{15}{89}\right) = -1$. We therefore conclude that 15 is not a square modulo 89.

Example 14. Find all primes p for which 5 is a square modulo p. Since $5 \equiv 1 \pmod 4$, we have by QRL, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. In $\mathbb{Z}_5$, the squares are $1^2 = 1, 2^2 = 4, 3^3 = 4, 4^4 - 1$. Hence we deduce that $p \equiv 1, 4 \pmod 5$.

Example 15. We now do a slightly more complicated example. Find all odd primes p such that 7 is a square modulo p.

Note that $7 \equiv 3 \pmod 4$. Since we wish to compute $\left(\frac{7}{p}\right)$ and use QRL so that $\left(\frac{7}{p}\right)$ is related to $\left(\frac{p}{7}\right)$, we need to look at two separate cases.

Case 1. Let $p \equiv 1 \pmod 4$. Then $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$. So, $\left(\frac{7}{p}\right) = 1$ iff $\left(\frac{p}{7}\right) = 1$. Now in $\mathbb{Z}_7$, the squares are $1, 2, 4$. Hence $p \equiv 1, 2, 4 \pmod 7$. Thus p has to satisfy simultaneously any one of the 3 pairs of congruences:

(i) $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 7$,

(ii) $p \equiv 1 \pmod 4$ and $p \equiv 2 \pmod 7$,
iii) $p \equiv 1 \pmod 4$ and $p \equiv 4 \pmod 7$.

The first of these entail $p \equiv 1 \pmod{28}$, by CRT.

In the AP, $4k+1$, $\{1, 5, 9, 13, 17, 21, 25, \ldots\}$, we find that 9 satisfies the second set of congruences while 25 satisfies the 3rd set. (You may also solve it by standard method, we took the easy way out! $4k+1 \equiv 2 \pmod 7$, that is, $4k \equiv 1 \pmod 7$ or $8k \equiv 2 \pmod 7$ which is same as $k \equiv 2 \pmod 7$. An obvious choice is 9.) Thus for each odd prime p in the set of primes satisfying $p \equiv 1, 9, 25 \pmod{28}$ we find that 7 is a square modulo p.

Case 2. let $p \equiv 3 \pmod 7$. In this case, $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$. So, 7 is a square modulo p iff p a non-square modulo 7. The nonsquares modulo 7 are 3,5,6. Hence p must satisfy any one of the three congruences: $p \equiv 3 \pmod 7$, $p \equiv 5 \pmod 7$, or $p \equiv 6 \pmod 7$. As earlier, this says that p has to simultaneously satisfy any one of there pairs of congruences. We leave the details to the reader. Proceeding as in case 1, we find that the sets of required primes in Case 2 are of the form $p \equiv 3 \pmod{28}$, $p \equiv 19 \pmod{28}$ and $p \equiv 27 \pmod{28}$.

Finally, 7 is a square modulo an odd prime p iff $p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$.

A theorem of Dirichlet says that that there exist infinitely any primes in any arithmetic progression $\{a + km : k \in \mathbb{Z}\}$ where $\gcd(a, m) = 1$. Thus there exist infinitely many odd primes p such that 7 is a square modulo p.

No account of the law of quadratic reciprocity is complete till we say something about $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$.

Lemma 16. *Let p be an odd prime. Then $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. In particular, we have*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{8}$$

Proof. This is immediate from Euler's criterion: $(-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right) \pmod p$. □

Lemma 17. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases} \tag{9}$$

Proof. This proof also uses Euler's criterion. It is easier to understand the proof by looking at some concrete examples.

Let $p = 13 \equiv 1 \pmod 4$. The idea is to take $\frac{p-1}{2}!$ and multiply it by $2^{\frac{p-1}{2}}$.

$$\begin{aligned} 2^6 \cdot 1 \cdot 2 \cdots 5 \cdot 6 &= (2 \cdot 4 \cdot 6) \times (8 \cdot 10 \cdot 12) \\ &= (2 \cdot 4 \cdot 6)(-5 \cdot -3 \cdot -1) \\ &= (-1)^3 \times 6!. \end{aligned}$$

Hence we conclude that $2^{\frac{p-1}{2}} = 2^6 = (-1)^{\frac{p-1}{4}} = (-1)^3$.

Let us work out the case where $p \equiv 1, 5 \pmod 8$.

$$\begin{aligned} 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! &= 2 \cdot 4 \cdot 6 \cdots (p-1) \\ &= \left[2 \cdot 4 \cdots (\frac{p-1}{2})\right] \left[(-\frac{p-3}{2}) \cdots (-5) \cdot (-3) \cdot (-1)\right] \\ &\equiv (-1)^{\frac{p-1}{4}} \left(\frac{p-1}{2}\right)! \qquad (\mathrm{mod}\, p). \end{aligned}$$

(How did we get $-\frac{p-3}{2}$? We wrote down the additive inverse of $\frac{p+1}{2}$ modulo $p-1$: $(p-1) - \frac{p+1}{2} = \frac{p-3}{2}$.)

If $p \equiv 3, 7 \pmod 8$, we proceed as above to get

$$\begin{aligned} 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! &= 2 \cdot 4 \cdot 6 \cdots (p-1) \\ &= \left[2 \cdot 4 \cdots (\frac{p-3}{2})\right] \left[(-\frac{p-1}{2}) \cdots (-5) \cdot (-3) \cdot (-1)\right] \\ &\equiv (-1)^{\frac{p+1}{4}} \left(\frac{p-1}{2}\right)! \qquad (\mathrm{mod}\, p). \end{aligned}$$

□

Ex. 18. (1) Show that $\left(\frac{13}{31}\right) = \left(\frac{-18}{31}\right) = -1$.
(2) Show that $X^2 - 43$ has a root in $\mathbb{Z}_{923}$.
(3) Compute $\left(\frac{-59}{131}\right)$. *Hint:* Can you think of an easier Legendre symbol?
(4) Is the polynomial $X^2 + 189$ irreducible in $\mathbb{Z}_{491}$?
(5) Show that there exist infinitely many primes of the form $4k+1$. *Hint:* Exploit Lemma 16.
(6) Prove that 3 is a square modulo an odd prime p iff $p \equiv \pm 1 \pmod{12}$. (7) Prove that -3 is a square modulo an odd prime p iff p is of the form $\mathrm{mod}\, p16$.
(7) Prove that there exist infinitely many primes of the form $6k+1$.

References

[1] G. Rosseau , *On the Quadratic Reciprocity Law*, J. Austral. Math. Soc. (Series A) **51**, 423-425, 1991.

[2] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer India Edition, 2004.