## Quadratic Reciprocity

developed from the theory of finite fields, as a series of exercises

If $p$ is a prime, then an element $x \in \mathbf{Z}/p\mathbf{Z} - \{0\}$ is called a *quadratic residue* if $(\exists y \in \mathbf{Z}/p\mathbf{Z} - \{0\})\ x = y^2$. One also, loosely, calls an integer $q$ not divisible by $p$ a ''quadratic residue modulo $p$'' if $\bar{q} \in \mathbf{Z}/p\mathbf{Z}$ is a quadratic residue.

Given $p$, we can clearly determine with a finite amount of work which elements of $\mathbf{Z}/p\mathbf{Z}$ are quadratic residues, and thus which elements of $\mathbf{Z}$ are quadratic residues modulo $p$; the latter set will be periodic with period $p$. But given $q \in \mathbf{Z}$, it is not evident whether there will be any pattern in the set of primes $p$ modulo which $q$ is a quadratic residue. We shall discover below that there is.

We begin the study of this question with a reduction:

**(1)** Let $p$ be an odd prime, $(\mathbf{Z}/p\mathbf{Z})^*$ the group of units of $\mathbf{Z}/p\mathbf{Z}$, and $(\mathbf{Z}/p\mathbf{Z})^{*2}$ the subgroup $\{x^2 \mid x \in (\mathbf{Z}/p\mathbf{Z})^*\}$. (i) Find $[(\mathbf{Z}/p\mathbf{Z})^* : (\mathbf{Z}/p\mathbf{Z})^{*2}]$. (ii) Show from this that one can determine, given two integers $r$ and $s$ relatively prime to $p$, whether $rs$ is a quadratic residue modulo $p$, if one knows whether $r$ is and whether $s$ is. (iii) Deduce that one can describe the set of primes modulo which an arbitrary integer $q$ is a quadratic residue if one can do this whenever $q$ is a prime, and also when $q = -1$.

Until further mention, $p$ and $q$ will be distinct *odd primes*. We shall establish below a relation between the conditions that $q$ be a quadratic residue modulo $p$, and that $p$ be a quadratic residue modulo $q$, known as the Law of Quadratic Reciprocity, by studying in *two* ways the question

(∗) Does the Galois group of the polynomial $x^q - 1$ over $\mathbf{Z}/p\mathbf{Z}$ act by even permutations of the roots of that polynomial?

and comparing the answers that we get. As noted in (1), we also need to investigate the cases $q = -1$ and $q = 2$. These will be dealt with subsequently.

The first of our approaches to (∗) will be based on the fact that the Galois group is generated by the map $a \mapsto a^p$; the second, on the use of the discriminant. For the first approach we begin with a general result on cyclic groups:

**(2)** If $\langle x \rangle$ is a finite cyclic group, and $y \in \langle x \rangle$, show that the map $z \mapsto zy$ is an even permutation of the elements of $\langle x \rangle$ if and only if $y$ is a square in $\langle x \rangle$.

For $p$, $q$ still as above, let $(\mathbf{Z}/p\mathbf{Z})(\zeta_q)$ be the extension of $\mathbf{Z}/p\mathbf{Z}$ by a primitive $q$th root of unity, $\zeta_q$.

**(3)** Show that the following conditions are equivalent:

(a) The $p$th-power map acts by an even permutation on $\langle \zeta_q \rangle \subseteq \mathbf{Z}/p\mathbf{Z}(\zeta_q)^*$.

(b) Multiplication by $p$ acts as an even permutation on the elements of $\mathbf{Z}/q\mathbf{Z}$.

(c) $p$ is a quadratic residue modulo $q$.

We have now related something that happens in characteristic $p$ and something that happens in characteristic $q$. But (a) is formulated, not in $\mathbf{Z}/p\mathbf{Z}$, but $(\mathbf{Z}/p\mathbf{Z})(\zeta_q)$. The next step is to reduce this to a computation in $\mathbf{Z}/p\mathbf{Z}$.

**(4)** Compute the discriminant of $x^q - 1$ in $\mathbf{Z}$. (Suggestion: Consider successively the relation among the following elements: $d = \Pi_{i<j}\,(\zeta_q^i - \zeta_q^j)^2$, $d' = \Pi_{i \neq j}\,(\zeta_q^i - \zeta_q^j)$, $d'' = \Pi_{i \neq j}\,(1 - \zeta_q^{j-i})$, $E(1) = \Pi_{i \neq 0}\,(1 - \zeta_q^i)$, $E(x) = \Pi_{i \neq 0}\,(x - \zeta_q^i)$. If you do it this way, be more precise than I have been about the ranges of $i$ and $j$. And be careful!)

**(5)** Obtain from (4) a necessary and sufficient condition for the Galois group of $(\mathbf{Z}/p\mathbf{Z})(\zeta_q)$ to act by even permutations on the roots of $x^q - 1$. In putting this criterion in the simplest possible form, recall that for nonzero elements $a$ and $b$ of a field, $a$ is a square if and only if $ab^2$ is a square.

**(6)** Comparing the results of (3) and (5), get a relation between $p$ being a quadratic residue modulo $q$ and $q$ being a quadratic residue modulo $p$, which holds whenever $q \equiv 1 \pmod 4$. Reversing the roles of $p$ and $q$, show that the same relation holds when $p \equiv 1 \pmod 4$.

To handle the remaining case, where both $p$ and $q$ are $\equiv 3 \pmod 4$, we discover that we need to know when $-1$ is a quadratic residue. This is something we wanted to find out anyway, so

**(7)** Show that $-1$ is a quadratic residue modulo $p$ if and only if the group $\mathbf{Z}_p^*$ has an element of order 4. Determine conditions for this to happen in terms of the order of this group, and hence in terms of $p$.

**(8)** Complete the incomplete result of (6). Note: this result, the Law of Quadratic Reciprocity, is often stated in terms of the *Legendre Symbol* $(\frac{n}{p})$, which is defined, for $p$ a prime, and $n$ an integer not divisible by $p$, to be $+1$ if $n$ is a quadratic residue modulo $p$, $-1$ if not. The special situation when $p, q \equiv 3 \pmod 4$ is expressed by bringing into the statement of the Law a term $(-1)^{((p-1)/2)((q-1)/2)}$.

As a practical application:

**(9)** Characterize the set of odd primes $p$ such that $-39$ is a quadratic residue modulo $p$ as those belonging to an explict list of congruence classes modulo some integer. Give all such primes $< 100$. (You need *not* find square roots of $-39$ modulo each!)

It remains to handle the case $q = 2$. Note that all fields $\mathbf{Z}/p\mathbf{Z}$ ($p$ odd) have a primitive square root of unity, namely $-1$, so the Galois group of $(\mathbf{Z}/p\mathbf{Z})(\zeta_2)$ is trivial; nevertheless, $2$ is a quadratic residue in some fields $\mathbf{Z}/p\mathbf{Z}$ but not in others. It turns out that, just as the case $q = -1$ involved the study of primitive 4th roots of 1, so the case $q = 2$ can be solved by considering primitive 8th roots of 1, as is suggested by the formula $\zeta_8 = (1+i)/\sqrt{2}$.

**(10)** Without assuming the above formula, show that in any field $K$ containing a primitive 8th root of unity $\zeta_8$, the element $\zeta_8 + \zeta_8^{-1}$ is a square root of 2. Taking $K = (\mathbf{Z}/p\mathbf{Z})(\zeta_8)$, deduce that $\mathbf{Z}/p\mathbf{Z}$ contains a square root of 2 if and only if $\zeta_8 + \zeta_8^{-1}$ is fixed under the $p$th-power automorphism. Determine for what values of $p$ this holds. (Hint: given any field $K$ with a primitive 8th root of unity $\zeta_8$, and an odd integer $n$, compare $\zeta_8 + \zeta_8^{-1}$ and $\zeta_8^{n} + \zeta_8^{-n}$.)

This completes the task we set ourselves to begin with. But one may generalize our question, and ask when an element of a larger field $\mathbf{F}_{p^n}$ is a square in that field. This is answered in

**(11)** Letting $\mathbf{F}_{p^n}$ denote the field of $p^n$ elements, show that the *norm* map: $\mathbf{F}_{p^n} \to \mathbf{Z}/p\mathbf{Z}$ is surjective. (This is essentially Hungerford's Exercise V.7.2.) Deduce that an element $a \in \mathbf{F}_{p^n}$ is a square in this field if and only if its norm in $\mathbf{Z}/p\mathbf{Z}$ is a quadratic residue.

There are other related questions which do not have such neat answers. For instance, given a prime $p$ one may ask whether *neither*, *one* or *both* of $4 \pm \sqrt{3}$ are squares in $(\mathbf{Z}/p\mathbf{Z})(\sqrt{3})$.

**(12)** Show (with the help of the preceding results) how to answer the above question in terms of congruences satisfied by $p$, in all cases *except* when 3 and $(4+\sqrt{3})(4-\sqrt{3}) = 13$ are both quadratic residues modulo $p$.

I am told by a number-theorist that in the case excluded above, the answer is not determined by congruences satisfied by $p$; however, from the fact that 3 is a quadratic residue mod $p$, it follows that there is a factorization $p = (a+\sqrt{3}b)(a-\sqrt{3}b)$ in $\mathbf{Z}[\sqrt{3}]$, and the question *can*, it seems, be answered in terms of congruences satisfied by the coefficients $a$ and $b$ in this factorization.

We end with an exercise which is tangential to the above results, and uses only (1) above:

**(13)** If $m$ and $n$ are integers, show that the polynomial $(x^2-m)(x^2-n)(x^2-mn)$ has a root in every field $\mathbf{Z}/p\mathbf{Z}$. By appropriate choice of $m$ and $n$, get an example of a polynomial in $\mathbf{Z}[x]$ having a root in every field of finite characteristic, but no root in $\mathbf{Q}$.