1. LEGENDRE, JACOBI, AND KRONECKER SYMBOLS

by Leo Goldmakher

1.1. **Legendre symbol.** Efficient algorithms for solving quadratic equations have been known for several millennia. However, the classical methods only apply to quadratic equations over $\mathbb{C}$; efficiently solving quadratic equations over a finite field is a much harder problem. For a typical integer a and an odd prime p, it's not even obvious a priori whether the congruence $x^2 \equiv a \pmod{p}$ has *any* solutions, much less what they are. By Fermat's Little Theorem and some thought, it can be seen that $a^{(p-1)/2} \equiv -1 \pmod{p}$ if and only if a is not a perfect square in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; otherwise, it is $\equiv 1$ (or 0, in the trivial case $a \equiv 0$). This provides a simple computational method of distinguishing squares from nonsquares in $\mathbb{F}_p$, and is the beginning of the *Miller-Rabin primality test*.

Motivated by this observation, Legendre introduced the following notation:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a nonzero solution} \\ -1 & \text{if } x^2 \equiv a \pmod{p} \text{ has no solutions.} \end{cases}$$

Note from above that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. The Legendre symbol $\left(\frac{a}{p}\right)$ enjoys several nice properties. Viewed as a function of a (for fixed p), it is a Dirichlet character (mod p), i.e. it is completely multiplicative and periodic with period p. Moreover, it satisfies a duality property: for any odd primes p and q,

$$\left(\frac{p}{q}\right) = \langle p, q \rangle \left(\frac{q}{p}\right) \tag{1}$$

where $\langle m, n \rangle = 1$ unless both m and n are $\equiv 3 \pmod{4}$, in which case $\langle m, n \rangle = -1$. The relation (1) is known as *quadratic reciprocity*, and its proof was one of Gauss' proudest achievements.

It can be shown that if one fixes a rather than p, the Legendre symbol depends only on the residue class of p in some finite group $(\mathbb{Z}/n\mathbb{Z})^*$, where n depends on a. For example,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv -1 \pmod{4} \end{cases} \qquad \left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

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

1.2. **Jacobi symbol.** It is convenient to extend the Legendre symbol $\left(\frac{a}{p}\right)$ to a symbol $\left(\frac{a}{b}\right)$, where b is an arbitrary odd integer; this generalization is called the *Jacobi symbol*. Whenever b is an odd prime, we take $\left(\frac{a}{b}\right)$ to be the Legendre symbol. We now extend this by multiplicativity to all positive odd integers b. In other words, if $b = p_1^{e_1} \cdots p_k^{e_k}$ where the p_i are odd primes, set

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}.$$

As usual with empty products, we set $\left(\frac{a}{1}\right) = 1$. We can further extend this to all odd negative integers b by setting $\left(\frac{a}{-1}\right) = \text{sgn}(a)$ for all nonzero a.

It can be checked that for fixed b and variable a, the Jacobi symbol is a Dirichlet character (mod $|b|$), so long as $|b| \geq 2$. It also satisfies a quadratic reciprocity law:

$$\left(\frac{a}{b}\right) = \langle a, b \rangle \left(\frac{b}{a}\right).$$

1.3. **Kronecker symbol.** We saw above that for a fixed odd integer b and arbitrary integer a, the Jacobi symbol $\left(\frac{a}{b}\right)$ gives a Dirichlet character (mod $|b|$). What if instead we fixed a and let b vary; is this, too, a Dirichlet character? After all, it's completely multiplicative by definition. One immediate difficulty is that the Jacobi symbol doesn't admit even values of b. One can formally circumvent this difficulty by defining the behavior of the symbol for $b = 0$ and $b = 2$ and extending to all integers b by multiplicativity. We must have $\left(\frac{a}{0}\right) = 0$ for the symbol $\left(\frac{a}{\cdot}\right)$ to stand a chance of being a character. Defining the symbol $\left(\frac{a}{2}\right)$ is more subtle, but taking a clue from the behavior of $\left(\frac{2}{p}\right)$ (described at the end of the first section) we might guess that a good choice is

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } 2 \mid a \\ 1 & \text{if } a \equiv \pm 1 \pmod 8 \\ -1 & \text{if } a \equiv \pm 3 \pmod 8. \end{cases}$$

Extending the Jacobi symbol by multiplicativity, we now have a symbol $\left(\frac{a}{b}\right)$ defined for all integers a and b; this is called the *Kronecker symbol*.

1.4. **Primitive quadratic characters.** As it turns out, one can give a simple characterization of the primitive quadratic characters in terms of the Kronecker symbol. We first recall that a *fundamental discriminant* is any integer which is the discriminant of some quadratic extension of $\mathbb{Q}$.

Theorem 1.1. *For every fundamental discriminant D, $\chi_D := \left(\frac{D}{\cdot}\right)$ is a primitive quadratic character of conductor $|D|$. Conversely, given any primitive quadratic character χ, there exists a unique fundamental discriminant D such that $\chi = \chi_D$.*

The proof of this theorem can be found in Section 2.2.4 of [1]. We make a few remarks.

- By convention, 1 is a fundamental discriminant, since it is the discriminant of the degenerate quadratic extension $K = \mathbb{Q}$. Appropriately, the corresponding character χ_1 is the principal character (mod 1). Note that χ_1 is the unique primitive principal character, as it induces all other principal characters.
- The set of fundamental discriminants can be explicitly determined. Recall that any quadratic extension $K/\mathbb{Q}$ can be written uniquely in the form $K = \mathbb{Q}(\sqrt{d})$ with $|d|$ squarefree. Then the discriminant of K is

  $$\text{disc}_K = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod 4 \end{cases}$$

  Thus for example the set of all fundamental discriminants of magnitude smaller than 16 is

  $$\{\ldots, -15, -11, -8, -7, -4, -3, 1, 5, 8, 12, 13, \ldots\}$$

- The theorem says nothing about χ_a when a is not a fundamental discriminant. Such χ_a might be primitive Dirichlet characters (e.g. χ_2), imprimitive characters (e.g. χ_4), or even not a character at all (e.g. χ_3).

We expand on the last remark above. The smallest integers which are not fundamental discriminants are ± 2. From our definition, it is easy to see that both of $\chi_{\pm 2}$ are primitive characters (mod 8):

$$\chi_2(n) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod 8 \\ -1 & \text{if } n \equiv \pm 3 \pmod 8 \end{cases} \qquad \chi_{-2}(n) = \begin{cases} 1 & \text{if } n \equiv 1, 3 \pmod 8 \\ -1 & \text{if } n \equiv -1, -3 \pmod 8 \end{cases}$$

At first sight, this seems to contradict our classification of primitive real characters. However, a little thought shows that each of these characters can be written in terms of a fundamental discriminant: $\chi_{\pm 2} = \chi_{\pm 8}$.

The remaining two characters (mod 8) are $\chi_{\pm 4}$. χ_4 is the principal character (mod 8), which also happens to the principal character (mod 2) and (mod 4). Note that it is imprimitive, being induced by the primitive principal character χ_1. χ_{-4} is the nonprincipal primitive character (mod 4); not a surprise, since -4 is a fundamental discriminant. Of course, when considered as a character (mod 8) it is imprimitive.

Thus, even when a is not the discriminant of a quadratic extension of $\mathbb{Q}$, the Kronecker symbol χ_a might be a primitive or imprimitive character. However, there's another possibility: that χ_a isn't a character at all. This is the case for χ_3, as we now show.

Proposition 1.2. *$\chi_3(2) = -1$ and $\chi_3(6k \pm 1) = (-1)^k$ for all integers k.*

Note that this proposition completely determines χ_3, since any integer is either a multiple of 3 or can be written uniquely in the form $2^\ell(6k \pm 1)$.

Corollary 1.3. *χ_3 is not a periodic function, and hence, not a character.*

Proof. Suppose χ_3 were periodic, with period $q > 0$. Then $\chi_3(q) = \chi_3(0) = 0$, whence $3 \mid q$. Write $q = 3k$. Then $1 = \chi_3(1 + 2q) = \chi_3(6k + 1) = (-1)^k$. This implies that k is even, i.e. that $6 \mid q$. We can now proceed by induction to prove that $2^\ell \times 6 \mid q$ for all $\ell \geq 0$. Indeed, suppose $2^\ell \times 6 \mid q$, say $q = 2^\ell \times 6k$. Then

$$\chi_3(2^\ell) = \chi_3(2^\ell + q) = \chi_3(2^\ell)\chi_3(1 + 6k) = (-1)^k \chi_3(2^\ell).$$

This shows that k must be even, whence $2^{\ell+1} \times 6 \mid q$. In particular, q is divisible by arbitrarily large powers of 2, which is impossible. □

1.5. **Questions.**

1.5.1. Write out an explicit definition of χ_1, à la the expressions for $\chi_{\pm 2}$ above.

1.5.2. In the text we saw that χ_3 is not a Dirichlet character. Find another a for which χ_a is not a character. What nice properties does χ_a have when it is not a Dirichlet character?

1.5.3. In the text, we saw that $\chi_{\pm 2}$ are primitive characters, despite the fact that neither ± 2 are fundamental discriminants. Can you find other such a, not fundamental discriminants, for which χ_a is a primitive Dirichlet character? What can you say about the set of all such a?

REFERENCES

[1] H. Cohen, *Number Theory*, Graduate Texts in Mathematics, vol. 239, Springer-Verlag, New York, 2007.
[2] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO,
ROOM 6290, 40 ST. GEORGE STREET
TORONTO, ONTARIO, CANADA M5S 2E4
E-mail address: lgoldmak@math.toronto.edu