QUADRATIC RESIDUES
(MA2316, FOURTH WEEK)

VLADIMIR DOTSENKO

An integer a is said to be a quadratic residue modulo p if the congruence $x^2 \equiv a \pmod p$ has solutions. We define the *Legendre symbol* $\left(\frac{a}{p}\right)$ of a modulo p by the formula

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ if } \gcd(a,p)=1 \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1, \text{ if } \gcd(a,p)=1 \text{ and } a \text{ is not a quadratic residue modulo } p, \\ 0, \text{ if } a \equiv 0 \pmod p. \end{cases}$$

Exercise. For an odd prime p, the number of solutions to the congruence $x^2 \equiv a \pmod p$ is equal to $1 + \left(\frac{a}{p}\right)$.

Proposition 1. *Let p be an odd prime. The number of quadratic residues in $(\mathbb{Z}/p\mathbb{Z})^\times$ is equal to $\frac{p-1}{2}$, that is half of nonzero integers modulo p are quadratic residues.*

Proof. We know that the multiplicative group modulo p is cyclic, $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, g, \ldots, g^{p-2}\}$ for some g, which implies that squares in it are precisely those g^i with even i (although i is defined modulo $p-1$, since p is odd, the parity of i is well defined). □

The description of quadratic residues in the previous proof implies that the product of two quadratic residues is a quadratic residue, the product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue, and the product of two quadratic nonresidues is a quadratic residue. In other words,

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

In fact, this statement can be improved a lot right away. Namely,

Proposition 2 (Euler's lemma)**.** *Let p be an odd prime. We have*

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

Proof. Let us consider the factorisation $x^{p-1} - 1 = (x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1)$. The roots of the left hand side are all nonzero elements modulo p, and each quadratic residue is manifestly a root of the first factor on the right. Since there are $\frac{p-1}{2}$ quadratic residues, and a polynomial of degree d over a field has at most d roots, we conclude that the roots of the first factor are precisely all quadratic residues, and the roots of the second factor are precisely all quadratic nonresidues. □

Exercise. Why is the proposition we just proved an "improvement" of the previous one?

Corollary. *Let p be an odd prime. We have*

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

Proof. The previous statement guarantees that the two are congruent modulo p. But both numbers are equal to ± 1, so they can be congruent modulo an odd prime if and only if they are equal. □

Theorem 1 (Quadratic reciprocity law)**.** *Let p and q be odd primes. Then* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Proof. The key ingredient in this proof is

Lemma (Zolotarev's lemma)**.** *Let p be an odd prime, and let a be an integer coprime to p. Consider the permutation σ_a of $1, 2, \ldots, p-1$ defined by multiplying everything by a and reducing modulo p. Then*

$$\left(\frac{a}{p}\right) = \operatorname{sign}(\sigma_a).$$

Proof. Note that the sign of a permutation σ of $1, \ldots, n$ can be defined by the property

$$\prod_{1\le i<j\le n} (x_{\sigma(i)} - x_{\sigma(j)}) = \operatorname{sign}(\sigma) \prod_{1\le i<j\le n} (x_i - x_j).$$

Let us put $n = p$, $\sigma = \sigma_a$, and $x_i = i$ for all $i = 1, \ldots, p$. Then we have

$$\operatorname{sign}(\sigma_a) \prod_{1\le i<j\le p} (i-j) = \prod_{1\le i<j\le p} (\sigma_a(i)-\sigma_a(j)) \equiv \prod_{1\le i<j\le p} (ai-aj) = a^{\frac{p(p-1)}{2}} \prod_{1\le i<j\le p} (i-j) \pmod p.$$

We conclude that

$$\operatorname{sign}(\sigma_a) \equiv a^{\frac{p(p-1)}{2}} \equiv (a^{\frac{(p-1)}{2}})^p \equiv \left(\frac{a}{p}\right)^p = \left(\frac{a}{p}\right) \pmod p.$$

But both numbers involved are equal to ± 1, so they may be congruent modulo an odd prime if and only if they are equal. □

To use Zolotarev's lemma, we shall invoke the Chinese Remainder Theorem. Let us consider the permutations λ, μ of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ defined by the formulas

$$\lambda(a, b) = (a, a + pb),$$
$$\mu(a, b) = (qa + b, b).$$

Clearly, λ permutes elements of the form (a_0, b) with the same a_0, and it easily follows that $\operatorname{sign}(\lambda) = \left(\frac{p}{q}\right)^p = \left(\frac{p}{q}\right)$. Similarly, $\operatorname{sign}(\mu) = \left(\frac{q}{p}\right)^q = \left(\frac{q}{p}\right)$.

Let us now consider the permulation ν of $\mathbb{Z}/(pq)\mathbb{Z}$ obtained as follows: we use the identification $\rho\colon \mathbb{Z}/(pq)\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$ (here we use the Chinese Remainder Theorem), and put $\nu = \rho^{-1}\mu\lambda^{-1}\rho$. In plain words, we have $\nu(a + pb) = qa + b$. Let us compute the sign of this permutation in two different ways. First, our previous computations show that $\operatorname{sign}(\nu) = \operatorname{sign}(\mu)\operatorname{sign}(\lambda^{-1}) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$. Second, we can try to compute this sign directly, counting the number of inversions, that is counting the number of pairs of pairs $((a, b), (a', b'))$ for which $a + pb < a' + pb'$ but $qa + b > qa' + b'$, that is $a - a' < p(b' - b)$ and $q(a - a') > b' - b$. This immediately implies that $a - a' > 0$ and $b - b' < 0$. (Indeed, combining these inequalities, we get $b' - b < q(a - a') < pq(b' - b)$ and $pq(a - a') > p(b' - b) > a - a'$). Therefore, the number of sought pairs of pairs is equal to $\binom{p}{2}\binom{q}{2} \equiv \frac{p-1}{2}\cdot\frac{q-1}{2} \pmod 2$, and therefore we have $\operatorname{sign}(\nu) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$, which completes the proof. □

In the next tutorial class, you will show that for an odd prime p, we have $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. This statement is often referred to a "supplement to quadratic reciprocity law", meaning that altogether this statement, the quadratic reciprocity law itself, and the formula for $\left(\frac{-1}{p}\right)$ that we proved, give a very fast way of computing Legendre symbols. For example,

$$\left(\frac{23}{103}\right) = -\left(\frac{103}{23}\right) = -\left(\frac{11}{23}\right) = \left(\frac{23}{11}\right) = \left(\frac{1}{11}\right) = 1,$$

$$\left(\frac{43}{101}\right) = \left(\frac{101}{43}\right) = \left(\frac{15}{43}\right) = \left(\frac{3}{43}\right)\left(\frac{5}{43}\right) = -\left(\frac{43}{3}\right)\left(\frac{43}{5}\right) = -\left(\frac{2}{3}\right)\left(\frac{3}{5}\right) = -(-1)(-1) = -1,$$

$$\left(\frac{253}{257}\right) = \left(\frac{-4}{257}\right) = \left(\frac{-1}{257}\right)\left(\frac{2}{257}\right)^2 = 1.$$