6. Quadratic residues

6.1 Quadratic residues

Assume that $p \geq 3$ is prime and that x is such that $1 \leq x \leq p-1$. For any integer a with $(a,p)=1$, there exists a unique x' with $1 \leq x' \leq p-1$ such that $xx' \equiv a \pmod{p}$.

Definition 6.1 We call x' the *associate of x with respect to a modulo p* if

$$xx' \equiv a \pmod{p}$$

with $1 \leq x' \leq p-1$.

We are in particular interested in the case where the associate of x is itself.

Definition 6.2 Let p be a prime and a be such that $(a,p)=1$. We say that a is a *quadratic residue modulo p* if there exists an x such that

$$x^2 \equiv a \pmod{p}.$$

We usually write $a \,\mathrm{R}\, p$ is this case. If such x does not exist, we say that a is a *quadratic non-residue modulo p*, and write $a \,\mathrm{N}\, p$.

Note that when $p=2$, for any a such that $(a,2)=1$, we always have $a \equiv 1 = 1^2 \pmod{2}$. Thus, all such a's are quadratic residues modulo 2. Below, we only focus on the case where $p \geq 3$.

Lemma 6.1 Let $p \geq 3$ be a prime and x_0 be such that $(x_0,p)=1$. Then

$$x^2 \equiv x_0^2 \pmod{p} \tag{6.1}$$

has exactly two solutions

$$x_+ \equiv x_0 \pmod{p} \qquad \text{and} \qquad x_- \equiv -x_0 \pmod{p},$$

and in particular $x_+ \not\equiv x_- \pmod{p}$.

Proof. We rewite (6.1) as

$$(x-x_0)(x+x_0) \equiv 0 \pmod{p}.$$

Since p is prime, it follows that $p \mid (x-x_0)$ or $p \mid (x+x_0)$, thereby leading to the two solutions $x_\pm$. Also, $x_+ \not\equiv x_- \pmod p$; otherwise, we have $x_0 \equiv -x_0 \pmod p$, or $p \mid 2x_0$, or $p \mid x_0$ since $p \geq 3$ is prime, which violates the assumption that $(x_0, p) = 1$. ■

Theorem 6.2 Let $p \geq 3$ be a prime.

(i) If a is a quadratic residue modulo p, then there are exactly two distinct residue classes $x \equiv x_1, x_2$ modulo p with $x_2 \equiv -x_1 \pmod p$ such that $x^2 \equiv a \pmod p$.

(ii) There are exactly $\frac{p-1}{2}$ quadratic residues modulo p, and $\frac{p-1}{2}$ quadratic non-residues modulo p. In particular, the quadratic residues can be represented by the residue classes $\{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$ modulo p.

Proof. (i). Since a is a quadratic residue, we may always find an x_1 such that $x_1^2 \equiv a \pmod p$. Thus, by Lemma 6.1, the only two solutions to $x^2 \equiv a \equiv x_1^2 \pmod p$ are $x \equiv \pm x_1 \pmod p$ and they are distinct.

(ii). First, Part (i) implies that there are at most $\frac{p-1}{2}$ quadratic residues modulo p. Otherwise, if there are $\geq \frac{p+1}{2}$ quadratic residues, then there are $\geq 2 \cdot \frac{p+1}{2} = p+1$ residue classes modulo p, which is impossible. Next, we show that $\{1^2, \ldots, (\frac{p-1}{2})^2\}$ are pairwise distinct residue classes modulo p. To see this, we choose $1 \leq i, j \leq \frac{p-1}{2}$ with $i \neq j$. We claim that $i^2 \not\equiv j^2 \pmod p$. Otherwise, if $i^2 \equiv j^2 \pmod p$, then $p \mid (i-j)(i+j)$. But since $1 \leq i, j \leq \frac{p-1}{2}$ and $i \neq j$, both $i-j$ and $i+j$ are not multiples of p, thereby leading to a contradiction. Thus, there are exactly $\frac{p-1}{2}$ quadratic residues modulo p, characterized by $\{1^2, \ldots, (\frac{p-1}{2})^2\}$ modulo p, and as a consequence, there are exactly $(p-1) - \frac{p-1}{2} = \frac{p-1}{2}$ quadratic non-residues modulo p. ■

Theorem 6.3 Let $p \geq 3$ be a prime.

(i) If a is a quadratic residue modulo p, then

$$(p-1)! \equiv -a^{\frac{p-1}{2}} \pmod p. \tag{6.2}$$

(ii) If a is a quadratic non-residue modulo p, then

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod p. \tag{6.3}$$

Proof. Recall that for each a with $(a, p) = 1$, every integer x with $1 \leq x \leq p-1$ has a unique associate x' (with respect to a modulo p) of one another with $1 \leq x' \leq p-1$.

For quadratic residues a, we know from Theorem 6.2(i) that there are exactly two x's, say $x = x_1$ and $x = p - x_1$, whose associate is itself. Therefore, we may group $\{1, \ldots, p-1\}$ into (x_1), $(p-x_1)$ and $\frac{p-3}{2}$ distinct unordered pairs (x, x') with

$$x_1^2 \equiv (p-x_1)^2 \equiv a \pmod p$$

and

$$xx' \equiv a \pmod p.$$

Thus,

$$(p-1)! = x_1 \cdot (p-x_1) \cdot \prod (xx') \equiv -x_1^2 \cdot \prod (xx') \equiv -a \cdot a^{\frac{p-3}{2}} = -a^{\frac{p-1}{2}} \pmod p.$$

For quadratic non-residues a, we cannot find any x such that $x^2 \equiv a \pmod p$. Therefore, we group $\{1, \ldots, p-1\}$ into $\frac{p-1}{2}$ distinct unordered pairs (x, x') with

$$xx' \equiv a \pmod p.$$

Thus,

$$(p-1)! = \prod (xx') \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

The proof is therefore complete. ■

6.2 Wilson's Theorem

Let us take a look at the special case $a = 1$ of Theorem 6.3, which is known as *Wilson's Theorem*.

Theorem 6.4 (Wilson's Theorem). Let p be a prime. Then

$$(p-1)! \equiv -1 \pmod{p}. \tag{6.4}$$

Proof. If $p = 2$, we simply have $1 \equiv -1 \pmod 2$, which is trivial. If p is an odd prime, then we note that 1 is a quadratic residue modulo p, for $1 \equiv 1^2 \pmod p$. Therefore, taking $a = 1$ in (6.2) yields (6.4). ■

Note that (6.4) is always false if the prime p is replaced by a composite.

Theorem 6.5 For $m \geq 2$, we have $(m-1)! \equiv -1 \pmod m$ if and only if m is prime.

Proof. The "if" part is exactly Wilson's Theorem. For the "only if" part, we assume that m is composite. Then m has a divisor d with $1 < d < m$. Thus, this d is among $2, \ldots, m-1$, and thus $d \mid (m-1)!$. This then implies that $d \nmid \big((m-1)!+1\big)$. But if $(m-1)! \equiv -1 \pmod m$, or equivalently, $m \mid \big((m-1)!+1\big)$, then all the divisors of m also divide $(m-1)!+1$, thereby leading to a contradiction. ■

6.3 Legendre symbol

We usually use the *Legendre symbol* to characterize whether an integer a is a quadratic residue modulo an odd prime p.

Definition 6.3 Let $p \geq 3$ be a prime and a be an integer. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined by

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

Theorem 6.6 Let $p \geq 3$ be a prime and a be such that $(a, p) = 1$. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{6.5}$$

Proof. Note that Theorem 6.3 can be understood as

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

On the other hand, Wilson's Theorem asserts that

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

The desired result therefore follows. ■

Theorem 6.7 Let $p \geq 3$ be a prime and m, n be integers. Then

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right). \tag{6.6}$$

Proof. If one of m and n is a multiple of p, so is mn. Thus, in this case,

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = 0.$$

Now, we assume that $(m,p) = (n,p) = 1$ and thus $(mn,p) = 1$. Then by Theorem 6.6,

$$\left(\frac{mn}{p}\right) \equiv (mn)^{\frac{p-1}{2}} = m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \pmod{p},$$

that is, $p \mid \left|\left(\frac{mn}{p}\right) - \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\right|$. However, the values of $\left(\frac{m}{p}\right)$, $\left(\frac{n}{p}\right)$ and $\left(\frac{mn}{p}\right)$ are taken from $\{-1,1\}$. Thus, $\left|\left(\frac{mn}{p}\right) - \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\right| \leq 2$, implying that $\left(\frac{mn}{p}\right) - \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = 0$, as desired. ■

R Given an arithmetic function $f : \mathbb{Z} \to \mathbb{C}$, we say that it is *completely multiplicative* if for any m and n,

$$f(mn) = f(m)f(n).$$

"Multiplicative" vs "Completely multiplicative": For completely multiplicative functions, the above relation holds true even if $(m,n) > 1$.

6.4 When is -1 a quadratic residue modulo p?

Theorem 6.8 Let $p \geq 3$ be a prime. Then

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{6.7}$$

In particulae, -1 is a quadratic residue modulo p if $p \equiv 1 \pmod 4$, and a quadratic non-residue modulo p if $p \equiv 3 \pmod 4$.

Proof. We know from Theorem 6.6 that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$, and thus (6.7) follows since $\left(\frac{-1}{p}\right)$ takes value from $\{-1,1\}$ for odd primes p. Finally, $\frac{p-1}{2}$ is even if $p \equiv 1 \pmod 4$, and odd if $p \equiv 3 \pmod 4$. ■

6.5 Starters for sums of squares

We prove two additional results based on the knowledge of quadratic residues; they will be used in our later study of the "sum of squares" problems.

Theorem 6.9 Let $p \geq 3$ be a prime such that $p \equiv 1 \pmod 4$. Then there exists an integer x such that

$$x^2 + 1 = mp$$

with $0 < m < p$.

Proof. For primes $p \equiv 1 \pmod 4$, Theorem 6.8 tells us that -1 is a quadratic residue modulo p. Thus, there exists an x among $1, \ldots, p-1$ such that

$$x^2 \equiv -1 \pmod p.$$

In particular, we may choose x with $1 \le x \le \frac{p-1}{2}$, for if x satisfies the above congruence, so does $p-x$. Finally, we have $0 < x^2+1 < \left(\frac{p}{2}\right)^2 + 1 < p^2$. Thus, $x^2+1 = mp$ with $0 < m < p$. ■

Theorem 6.10 Let $p \ge 3$ be a prime. Then there exist integers x and y such that

$$x^2 + y^2 + 1 = mp$$

with $0 < m < p$.

Proof. Consider the following $p+1$ integers: x^2 for $0 \le x \le \frac{p-1}{2}$ and $-(y^2+1)$ for $0 \le y \le \frac{p-1}{2}$. Since there are p residue classes modulo p, by the pigeonhole principle, at least two of the $p+1$ integers fall into the same residue class. Note that all the x^2's are incongruent modulo p, and so are the $-(y^2+1)$'s. Thus, the two integers falling into the same residue class must be one x^2 and one $-(y^2+1)$. That is, there exists x and y with $0 \le x, y \le \frac{p-1}{2}$ such that $x^2 \equiv -(y^2+1) \pmod p$, or $x^2 + y^2 + 1 = mp$ for an integer m. Finally, we have $0 < 1 + x^2 + y^2 < 1 + 2\left(\frac{p}{2}\right)^2 < p^2$. Thus, $0 < m < p$. ■