Section 11

Quadratic Congruences

Week 8

A **quadratic congruence** is a congruence of the form

$$Ax^2 + Bx + C \equiv 0 \pmod{p},$$

where in this section p is an odd prime, and $A \not\equiv 0 \pmod{p}$. (Why?)

The aim in the next two sections is to determine when a quadratic congruence modulo a prime has a solution. This is not nearly as easy as to determine when a linear congruence has a solution.

As in the case of linear congruences, a solution to a quadratic congruence $\pmod{m}$ is a least residue $\pmod{m}$.

We begin by writing the above congruence in a simpler form.

11.1 Simple Form of a Quadratic Congruence

Example: Reduce the congruence $2x^2 + 3x + 1 \equiv 0 \pmod{5}$ to a congruence of the form $y^2 \equiv a \pmod{p}$.

Solution

Since $(2, 5) = 1$, the congruence $2x \equiv 1 \pmod{5}$ has a (unique) solution, namely 3. Thus the above congruence is equivalent to

$$3 \cdot 2x^2 + 3 \cdot 3x + 3 \cdot 1 \equiv 3 \cdot 0 \pmod{5},$$

i.e. $$x^2 + 4x + 3 \equiv 0 \pmod{5}.$$

Completing the square, we obtain

$$x^2 + 4x + (\tfrac{4}{2})^2 - (\tfrac{4}{2})^2 + 3 \equiv 0 \pmod{5},$$

i.e.

$$(x+2)^2 \equiv 1 \pmod{5}$$

i.e.

$$y^2 \equiv 1 \pmod{5}$$

where $y = x + 2$. The solutions are $y \equiv \pm 1 \pmod{5}$, hence $x \equiv 2, 4 \pmod{5}$. (Test!)

Hence we only need to consider quadratic congruences of the form $x^2 \equiv a \pmod{p}$.

11.2 Number of Solutions of Quadratic Congruences

Theorem 11.1 *If p is an odd prime and p does not divide a (thus $a \not\equiv 0 \pmod{p}$), then $x^2 \equiv a \pmod{p}$ has exactly two solutions, or no solutions at all.*

Proof.
Suppose the congruence has a solution; say r is a solution. Then $p - r$ is also a solution, because

$$(p-r)^2 \equiv p^2 - 2rp + r^2 \equiv r^2 \equiv a \pmod{p}.$$

Also, $p - r \not\equiv r \pmod{p}$, for if $p - r \equiv r \pmod{p}$, then $p - r = r$ (both are least residues), hence $p = 2r$, which is impossible because p is odd.

So r and $p - r$ are two distinct solutions.

Suppose s is any solution. Then

$$a \equiv r^2 \equiv s^2 \pmod{p},$$

so $p | (r^2 - s^2)$, that is, $p | (r-s)(r+s)$. Since p is prime,

$$p | (r-s) \quad \text{or} \quad p | (r+s).$$

In the first case, $s \equiv r \pmod{p}$ and in the second case, $s \equiv p - r \pmod{p}$. Since r, s and $p - r$ are least residues, it follows that $s = r$ or $s = p - r$. Thus r and $p - r$ are the only solutions. ■

- Note that $x^2 \equiv 0 \pmod{p}$ has only the solution $x \equiv 0 \pmod{p}$.
- It is also obvious that if $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ both have solutions and $a \not\equiv b \pmod{p}$, then the solutions of the first congruence are both different from the solutions of the second.
- On the other hand, the numbers 1^2, 2^2, ..., $(p-1)^2$ all exist, so each number $1, 2, ..., p-1$ is a solution to a congruence $x^2 \equiv a \pmod{p}$.

- Thus if a is selected from the integers $1, 2, ..., p-1$, then $x^2 \equiv a \pmod{p}$ will have two solutions for $\frac{p-1}{2}$ values of a and no solutions for the other $\frac{p-1}{2}$ values of a.

For example,

x	1	2	3	4	5	6	7	8	9	10	11	12
$x^2 \pmod{13}$	1	4	9	3	12	10	10	12	3	9	4	1

So if $p = 13$, then $x^2 \equiv a \pmod{13}$ has two solutions if $a \in \{1, 4, 3, 9, 10, 12\}$ and no solutions if $a \in \{2, 5, 6, 7, 8, 11\}$.

11.3 Quadratic Residues and Nonresidues

Definitions

- If $x^2 \equiv a \pmod{m}$ has a solution, then a is called a **quadratic residue** $\pmod{m}$.
- If $x^2 \equiv a \pmod{m}$ does not have a solution, then a is called a **quadratic nonresidue** $\pmod{m}$.

$\boxed{?}$ How do we tell the values of a for which there is a solution (the quadratic residues) apart from those for which there is none (the quadratic nonresidues)?

We often shorten the terms quadratic residue and quadratic nonresidue to residue and nonresidue, respectively.

Before we prove a result which would answer the above question, consider the following remarks about the odd prime p and integer a such that $(a, p) = 1$.

R1. By Fermat's Theorem (Theorem 6.1), $a^{p-1} \equiv 1 \pmod{p}$.

R2. Since p is odd, $p - 1$ is even and so $(p-1)/2 \in \mathbb{Z}^+$.

R3. The congruence $x^2 \equiv 1 \pmod{p}$ has exactly two solutions: $x = 1$ and $x = p-1$ (Lemma 6.2).

R4. The prime p has a primitive root g (Theorem 10.7), and the smallest integer t such that $g^t \equiv 1 \pmod{p}$ is, by definition, $t = p - 1$.

11.4 Euler's Criterion

Theorem 11.2 (Euler's Criterion) *If p is an odd prime and $p \nmid a$, then $x^2 \equiv a \pmod{p}$*

- *has a solution (i.e. a is a quadratic residue) if and only if*
$$a^{(p-1)/2} \equiv 1 \pmod{p};$$
- *has no solution (i.e. a is a quadratic nonresidue) if and only if*
$$a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Proof.
Let g be a primitive root of the odd prime p. Then $\operatorname{ord}_p g = \phi(p) = p-1$, so $g^t \not\equiv 1 \pmod{p}$ for any positive integer $t < p-1$. In particular, from Remarks (R1) – (R3) above, the congruence
$$g^{p-1} \equiv (g^{(p-1)/2})^2 \equiv 1 \pmod{p}$$
implies that
$$g^{(p-1)/2} \equiv 1 \pmod{p} \text{ or } g^{(p-1)/2} \equiv -1 \pmod{p}.$$
But the first case is impossible by R4. Thus
$$g^{(p-1)/2} \equiv -1 \pmod{p}. \tag{11.1}$$
Since $(a,p) = 1$, $a \equiv g^k \pmod{p}$ for some $k \in \{1, 2, ..., p-1\}$ (Theorem 10.6).

- If k is even, then $k/2$ is an integer. Then $x^2 \equiv a \pmod{p}$ has a solution, for we may let x be the least residue of $g^{k/2}$; moreover,
$$a^{(p-1)/2} \equiv (g^k)^{(p-1)/2} \equiv (g^{p-1})^{k/2} \equiv 1 \pmod{p}.$$
- If k is odd, then
$$\begin{aligned} a^{(p-1)/2} &\equiv (g^k)^{(p-1)/2} \equiv (g^{(p-1)/2})^k \equiv (-1)^k \quad \text{(from (11.1))} \\ &\equiv -1 \pmod{p}. \end{aligned} \tag{11.2}$$

Moreover, $x^2 \equiv a \pmod{p}$ does not have a solution: if r were a solution, then r would be a least residue $(\text{mod } p)$, thus $p \nmid r$, and we would have
$$\begin{aligned} 1 &\equiv r^{p-1} \pmod{p} && \text{(by Fermat's Theorem (Theorem 6.1)} \\ &\equiv (r^2)^{(p-1)/2} \equiv a^{(p-1)/2} \equiv -1 \pmod{p}, && \text{(from (11.2))} \end{aligned}$$
which is impossible. ■

♣ From Euler's Criterion we deduce that

if g is a primitive root of p, then g is a quadratic nonresidue of p,

because $\operatorname{ord}_p g = p - 1$ and so $g^{(p-1)/2} \equiv -1 \pmod{p}$.

Example: Use Euler's Criterion to show that $x^2 \equiv 5 \pmod{61}$ has a solution, and find the two solutions.

Solution

We need to calculate $5^{30} \pmod{61}$. Now,

$$\begin{aligned} 5^2 &\equiv 25 \pmod{61}, \\ 5^4 &\equiv 25^2 \equiv 15 \pmod{61}, \\ 5^8 &\equiv 15^2 \equiv 42 \pmod{61}, \\ 5^{16} &\equiv 42^2 \equiv 56 \pmod{61}, \\ 5^{32} &\equiv 56^2 \equiv 25 \pmod{61}. \end{aligned}$$

Since $(5, 61) = 1$, we may divide by $5^2 \equiv 25 \pmod{61}$ and so we get

$$5^{30} \equiv 1 \pmod{61}.$$

Thus the congruence has a solution. Now,

to solve $x^2 \equiv 5 \pmod{61}$, we add multiples of 61 to 5 and factor any squares:

$$\begin{aligned} x^2 &\equiv 5 \equiv 66 \equiv 127 \equiv 188 \equiv 2^2 \cdot 47 \pmod{61}, \\ 47 &\equiv 108 \equiv 6^2 \cdot 3 \pmod{61}, \\ 3 &\equiv 64 \equiv 8^2 \pmod{61}, \end{aligned}$$

hence

$$x^2 \equiv 2^2 6^2 8^2 \equiv 96^2 \equiv 35^2 \pmod{61}.$$

Thus $x \equiv \pm 35 \pmod{61}$ and the two solutions are 35 and $61 - 35 = 26$.

11.5 The Legendre Symbol

In theory, Euler's Criterion tells us exactly which quadratic congruences have solutions and which don't, but in practice it is hard to compute $a^{(p-1)/2} \pmod{p}$. There is an easier way (but it was difficult to find), for which we need the following definition.

Definition. The **Legendre symbol** (a/p) (pronounced "a above p"), where p is an odd prime and $p \nmid a$, is defined by

$$(a/p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \pmod{p} \\ -1 & \text{if } a \text{ is a quadratic nonresidue} \pmod{p}. \end{cases}$$

Thus from Euler's criterion,

$$(a/p) \equiv a^{(p-1)/2} \pmod{p}.$$

Theorem 11.3 *The Legendre symbol has the properties*

(A) *if* $a \equiv b \pmod{p}$, *then* $(a/p) = (b/p)$,
(B) *if* p *does not divide* a, *then* $(a^2/p) = 1$,
(C) *if* p *divides neither* a *nor* b, *then* $(ab/p) = (a/p)(b/p)$.

Proof.
(A): Combining Legendre symbols and Euler's Criterion, we see that

$$(a/p) \equiv a^{(p-1)/2} \pmod{p}. \tag{11.3}$$

Therefore if $a \equiv b \pmod{p}$, then

$$(a/p) \equiv a^{(p-1)/2} \equiv b^{(p-1)/2} \equiv (b/p) \pmod{p}.$$

But (a/p) and (b/p) are equal to either 1 or -1, thus it follows that $(a/p) = (b/p)$.

(B): Clearly, $x^2 \equiv a^2 \pmod{p}$ has a solution, namely the least residue of $a \pmod{p}$.

(C): From (11.3),

$$(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv (a/p)(b/p) \pmod{p}.$$

This shows that $(ab/p) \equiv (a/p)(b/p) \pmod{p}$, and since either side of the congruence is equal to either 1 or -1, it follows that $(ab/p) = (a/p)(b/p)$. ∎

Note that (C) implies that

the product of two residues is a residue,

the product of two nonresidues is a residue and

the product of a residue and a nonresidue is a nonresidue.

Example: Evaluate (19/5).

Solution
By (A), $(19/5) = (4/5)$ and by (B), $(4/5) = 1$.

Example: Given that $(2/17) = 1$, evaluate $(8/17)$.

Solution
By (C) and then (A), $(8/17) = (2/17)(4/17) = 1 \cdot 1 = 1$.

11.6 Evaluating Legendre Symbols

Using Theorem 11.3 we can evaluate some Legendre symbols, but how do we evaluate $(17/23)$, for example? We cannot at this stage reduce it any further, but suppose we knew how $(17/23)$ was related to $(23/17)$. Since $(23/17) = (6/17) = (2/17)(3/17)$, we would then only need to know $(2/17)$ and $(3/17)$, which (as we'll see) are relatively easy to find. The relationship between (p/q) and (q/p) is given by the **Quadratic Reciprocity Theorem**.

Theorem 11.4 (The Quadratic Reciprocity Theorem) *Let p and q be odd primes. If $p \equiv q \equiv 3 \pmod 4$, then $(p/q) = -(q/p)$, otherwise, $(p/q) = (q/p)$.*

We next give the formulas for $(-1/p)$ and $(2/p)$.

Theorem 11.5 *If p is an odd prime, then*

$$(-1/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Thus -1 is a quadratic residue of primes congruent to $1 \pmod 4$ and a quadratic nonresidue of primes congruent to $3 \pmod 4$.

Proof.
By Euler's criterion,

$$(-1/p) \equiv (-1)^{(p-1)/2} \pmod p.$$

If $p \equiv 1 \pmod 4$, then $p-1 \equiv 0 \pmod 4$, hence $(p-1)/2$ is even and $(-1)^{(p-1)/2} \equiv 1 \pmod p$. If $p \equiv 3 \pmod 4$, then $p - 1 \equiv 2 \pmod 4$, hence $(p-1)/2 \equiv 1 \pmod 2$, so $(p-1)/2$ is odd and $(-1)^{(p-1)/2} \equiv -1 \pmod p$. ■

Theorem 11.6 (To be proved in the next section.) *If p is an odd prime, then*

$$(2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8, \quad \text{i.e. if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8, \quad \text{i.e. if } p \equiv \pm 3 \pmod 8. \end{cases}$$

- Theorems 11.3 – 11.6 enable us to evaluate any Legendre symbol, thus to determine whether a is a quadratic residue of p for any a and any odd prime p.

Example: Determine whether $x^2 \equiv 1234 \pmod{4567}$ has a solution.

Solution

We must evaluate $(1234/4567)$. Note that $4567 \equiv 7 \pmod 8$. Using Theorems 11.3 – 11.6, we get

$$
\begin{array}{rcll}
(1234/4567) & = & (2/4567)(617/4567) & \text{Thm 11.3(C)} \\
 & = & (1)(617/4567) & \text{Thm 11.6, since } 4567 \equiv 7 \pmod{8} \\
 & = & (4567/617) & \text{QRT, since } 617 \equiv 1 \pmod{4} \\
 & = & (248/617) & \text{Thm 11.3(A)} \\
 & = & (2/617)(2^2/617)(31/617) & \text{Thm 11.3(C)} \\
 & = & (1)(1)(31/617) & \text{Thm 11.6 and Thm 11.3(B)} \\
 & = & (617/31) & \text{QRT, since } 617 \equiv 1 \pmod{4} \\
 & = & (28/31) & \text{Thm 11.3(A)} \\
 & = & (2^2/31)(7/31) & \text{Thm 11.3(C)} \\
 & = & (1)(-1)(31/7) & \text{Thm 11.3(B) and QRT} \\
 & = & -(3/7) & \text{Thm 11.3(A)} \\
 & = & (7/3) & \text{QRT, since } 7 \equiv 3 \pmod{4} \\
 & = & (1/3) & \text{Thm 11.3(A)} \\
 & = & 1 & \text{Thm 11.3(B)}
\end{array}
$$

Thus the congruence has a solution.

Section 12

Quadratic Reciprocity

The aim in this section is to prove Theorem 11.6, which gives the values of $(2/p)$ for the different residue classes of $p \pmod 8$. We need a result by Gauss, called Gauss's Lemma.

12.1 Gauss's Lemma

Example: Let $p = 17$. We know that $(2/17) = 1$ because $17 \equiv 1 \pmod 8$. Consider the least residues $\pmod{17}$ of

$$1 \cdot 2, \quad 2 \cdot 2, \quad 3 \cdot 2, ..., \quad 8 \cdot 2 = \tfrac{17-1}{2} \cdot 2.$$

They are $2, \ 4, \ 6, ..., \ 16$. How many of them are greater than $\frac{17-1}{2} = 8$? Four (an even number): 10, 12, 14, 16.

We also know that $(3/17) = (17/3) = (2/3) = -1$ because $3 \equiv 3 \pmod 8$. Consider the least residues $\pmod{17}$ of

$$1 \cdot 3, \quad 2 \cdot 3, \quad 3 \cdot 3, ..., \quad 8 \cdot 3 = \tfrac{17-1}{2} \cdot 3.$$

They are $3, \ 6, \ 9, \ 12, \ 15, \ 1, \ 4, \ 7$. How many of them are greater than $\frac{17-1}{2} = 8$? Three (an odd number): 9, 12, 15. This gives yet another way of distinguishing between quadratic residues and nonresidues of the odd prime p.

Theorem 12.1 (Gauss's Lemma) *Suppose p is an odd prime, $(a, p) = 1$ and amongst the least residues $\pmod p$ of*

$$a, \ 2a, \ 3a, ..., \ \left(\tfrac{p-1}{2}\right)a$$

there are exactly γ that are greater than $\frac{p-1}{2}$. Then $x^2 \equiv a \pmod p$ has a solution or not, depending on whether γ is even or odd. That is,

$$(a/p) = (-1)^{\gamma}.$$

Proof.
Let

$$r_1,\ r_2,\ \ldots,\ r_k$$

denote the least residues (mod p) of

$$a,\ 2a,\ 3a, \ldots,\ \left(\tfrac{p-1}{2}\right)a$$

that are less than or equal to $\frac{p-1}{2}$ and let

$$s_1,\ s_2,\ \ldots,\ s_\gamma$$

denote those that are greater than $\frac{p-1}{2}$. Thus $k + \gamma = \frac{p-1}{2}$.
Note that if $(p-1)/2 < s \leq p-1$, i.e. if $(p+1)/2 \leq s \leq p-1$, then $1 \leq p - s \leq ((p-1)/2)$.
Consider the set of numbers

$$r_1,\ r_2, \ldots,\ r_k,\ p - s_1,\ p - s_2,\ \ldots,\ p - s_\gamma. \tag{12.1}$$

There are $k + \gamma = \frac{p-1}{2}$ numbers in (12.1) and they all lie between 1 and $\frac{p-1}{2}$ (inclusive).

- We show that all $\frac{p-1}{2}$ numbers in (12.1) are distinct. Since they all lie between 1 and $\frac{p-1}{2}$, it will follow that they are a rearrangement of $1,\ 2, \ldots,\ \left(\frac{p-1}{2}\right)$.

  ⋆ Firstly, all the r_i are different:
  This follows because the congruence $ax \equiv r_i \pmod p$, p prime, has exactly one solution (Lemma 5.2). (Thus if $ka \equiv ma \equiv r_i \pmod p$, then $k = m$.)

  ⋆ Similarly, all the s_j are different and so all the $p - s_j$ are different.

  ⋆ For any i and j, $r_i \neq p - s_j$.
  Suppose to the contrary that for an i and a j,

  $$r_i = p - s_j.$$

  Then

  $$r_i + s_j \equiv p \equiv 0 \pmod p.$$

  But $r_i \equiv t_1 a \pmod p$ and $s_j \equiv t_2 a \pmod p$, where $1 \leq t_1, t_2 \leq \frac{p-1}{2}$. Hence

  $$t_1 a + t_2 a \equiv (t_1 + t_2)a \equiv 0 \pmod p,$$

  and since $(a, p) = 1$, it follows that

  $$t_1 + t_2 \equiv 0 \pmod p.$$

  But this is impossible since $1 \leq t_1, t_2 \leq \frac{p-1}{2}$ implies that

  $$2 \leq t_1 + t_2 \leq p - 1.$$

It follows that the $\frac{p-1}{2}$ numbers in (12.1) are all different and thus they are a rearrangement of

$$1,\ 2, ...,\ \left(\tfrac{p-1}{2}\right).$$

Form their product. Thus

$$r_1 r_2 \cdots r_k (p - s_1)(p - s_2) \cdots (p - s_\gamma) = 1 \times 2 \times \cdots \times \left(\tfrac{p-1}{2}\right). \tag{12.2}$$

But $p - s_j \equiv -s_j \pmod{p}$ and there are γ terms of this type. Thus (12.2) becomes

$$r_1 r_2 \cdots r_k s_1 s_2 \cdots s_\gamma (-1)^\gamma \equiv \left(\tfrac{p-1}{2}\right)! \pmod{p}. \tag{12.3}$$

But the r_i and s_j are by definition the least residues of $a,\ 2a,\ 3a, ...,\ \left(\frac{p-1}{2}\right)a \pmod{p}$ in some order, so the left hand side of (12.3) is congruent to

$$\begin{aligned}(a)(2a)(3a)\cdots\left(\left(\tfrac{p-1}{2}\right)a\right)(-1)^\gamma &\equiv 1 \times 2 \times \cdots \times \left(\tfrac{p-1}{2}\right) a^{(p-1)/2}(-1)^\gamma \\ &\equiv \left(\tfrac{p-1}{2}\right)!\ a^{(p-1)/2}(-1)^\gamma \pmod{p}.\end{aligned}$$

Thus from (12.3),

$$\left(\tfrac{p-1}{2}\right)! a^{(p-1)/2}(-1)^\gamma \equiv \left(\tfrac{p-1}{2}\right)! \pmod{p}.$$

The common factor $\left(\frac{p-1}{2}\right)!$ is relatively prime to p and may be cancelled to give

$$a^{(p-1)/2}(-1)^\gamma \equiv 1 \pmod{p}.$$

Multiplying both sides of the congruence with $(-1)^\gamma$, we get

$$a^{(p-1)/2}(-1)^{2\gamma} \equiv a^{(p-1)/2} \equiv (-1)^\gamma \pmod{p}.$$

Thus from Euler's Criterion,

$$(a/p) \equiv (-1)^\gamma \pmod{p}$$

and as (a/p) and $(-1)^\gamma$ are both either 1 or -1, this congruence implies equality. ■