Section 11. Quadratic Congruences

Note. In this section we consider congruences of the form $Ax^2+Bx+C \equiv 0 \pmod{m}$, where we require that m is an odd prime and $A \not\equiv 0 \pmod{m}$.

Note. With p prime, for any $A \not\equiv 0 \pmod{p}$ there is A' such that $AA' \equiv 1 \pmod{p}$ by Lemma 5.2. So the quadratic congruence $Ax^2 + Bx + C \equiv 0 \pmod{p}$ can always be converted to a quadratic congruence of the form $x^2+(A'B)x+(A'C) \equiv 0 \pmod{p}$.

Note. If $A'B$ is even, then we can complete the square in $x^2+(A'B)x+(A'C) \equiv 0 \pmod{p}$ to get

$$x^2 + (A'B)x + \left(\frac{A'B}{2}\right)^2 \equiv \left(\frac{A'B}{2}\right)^2 - (A'C) \pmod{p},$$

or

$$\left(x + \frac{A'B}{2}\right)^2 \equiv \left(\frac{A'B}{2}\right)^2 - (A'C) \pmod{p}.$$

If $A'B$ is odd, we can change it to $p + (A'B)$, which is even and of course $p \equiv 0 \pmod{p}$, and then complete the square. This gives $x^2 + (A'B + p)x + (A'C) \equiv 0 \pmod{p}$, from which we find

$$\left(x + \frac{A'B+p}{2}\right)^2 \equiv \left(\frac{A'B}{2} + p\right)^2 - (A'C) \pmod{p}.$$

Independent of the parity of $A'B$, we get an equivalent congruence of the form $y^2 \equiv a \pmod{p}$. So if we can solve this congruence, then we can solve any quadratic congruence (mod p); we still require $p \neq 2$.

Exercises 11.1, 11.2, and 11.3. Consider the quadratic congruence $2x^2+3x+1 \equiv 0 \pmod{5}$. Convert is to a quadratic with x^2 coefficient 1. Then change the congruence into the form $y^2 \equiv a \pmod{p}$. Find all solutions.

Solution. For $A = 2$ and $p = 5$, we need $A' = 3$ since $A'A = 2 \cdot 3 \equiv 1 \pmod{5}$. So the original congruence becomes $3 \cdot (2x^2 + 3x + 1) \equiv 0 \pmod{5}$ or $\boxed{x^2 + 4x + 3 \equiv 0 \pmod{5}}$. Since $A'B \equiv 4 \pmod{5}$ is even, then $A'B/2 \equiv 2 \pmod{5}$ and we complete the square to get $(x + (2))^2 \equiv (2) - 1 \equiv 1 \pmod{5}$, or $\boxed{y^2 \equiv (x + 2)^2 \equiv 1 \pmod{5}}$. By inspection, we see that the possible values of y are 1 or 4 (mod 5), so that the values of x are $\boxed{2 \text{ or } 4 \pmod{5}}$. □

Note. Continuing along similar lines of the previous exercises, notice that not all quadratic congruences have solutions. With $p = 5$, we have for the least residues modulo 5 that $0^0 \equiv 0 \pmod{5}$, $1^2 \equiv 4^2 \equiv 1 \pmod{5}$, and $2^2 \equiv 3^2 \equiv 4 \pmod{5}$. So the quadratic congruence $x^2 \equiv a \pmod{5}$ has no solution for $a = 2$ or 3. Also, there is one solution when $a = 0$, and two solutions for $a = 1$ or 4. We would expect two solutions to a quadratic (by the Fundamental Theorem of Algebra, say), and we see that if $r^2 \equiv 2 \pmod{p}$, then $(-r)^2 \equiv (p-r)^2 \equiv p^2 - 2pr + r^2 \equiv r^2 \equiv a \pmod{p}$. So if r is a least residue modulo p that is a solution to $x^2 \equiv a \pmod{p}$, then so is least residue $p - r$; this gives two different solutions unless $r \equiv 0 \pmod{p}$ in which case $p - r \equiv r \equiv 0 \pmod{p}$. The next theorem classifies the number of solutions.

Theorem 11.1. Suppose that p is an odd prime. If $p \nmid a$, then $x^2 \equiv a \pmod{p}$ has exactly two (least residue) solutions or no solutions.

Note. The condition that p if prime is necessary in Theorem 11.1. For example, the quadratic congruence $x^2 \equiv 1 \pmod{8}$ has more than two solutions, namely 1, 3, 5, and 7.

Note. As shown in the proof of Theorem 11.1, if r is a solution to $x^2 \equiv a$ (mod p) then $p - r$ (where $r \not\equiv p - r \pmod{p}$) is also a solution, and these are the only solutions. So we can pair together the least residues $1, 2, 3, \ldots, p-1$ in such a way that they give solutions to $x^2 \equiv a \pmod{p}$, with each pair associated with a different value of a. So for the possible values $1, 2, 3, \ldots, p-1$ of a, half of them are associated with quadratic congruences that have two solutions, and the other half are associated with quadratic congruences that have no solutions. That is, the quadratic congruence $x^2 \equiv a \pmod{p}$ has two solutions for $(p-1)/2$ of the values of a, and has no solutions for the other $(p-1)/2$ values of a. For example, with $p = 7$ the various values of x give:

x	1	2	3	4	5	6
$x^2 \pmod{7}$	1	4	2	2	4	1

Notice the values of $x^2 \pmod{7}$ are symmetric in the table with respect to $p/2 = 7/2 = 3.5$, because the value of r^2 is the same as the value of $(p-r)^2$. The values of a here for which two solutions exist are 1, 2, and 4. The next theorem gives a condition on a that allows us to determine if the quadratic congruence has two solutions or no solutions.

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 or no solution depending on whether $a^{(p-1)/2} \equiv 1 \pmod{p}$, or $a^{(p-1)/2} \equiv -1 \pmod{p}$, respectively.

Definition. If $x^2 \equiv a \pmod{m}$ has a solution, then a is a *quadratic residue* (mod m). If $x^2 \equiv a \pmod{m}$ has no solution, then a is a *quadratic nonresidue* (mod m). We similarly consider $x^n \equiv a \pmod{m}$ and define an nth residue and nth nonresidue.

Problem 11.2(b). Does $x^2 \equiv 15 \pmod{31}$ have a solution?

Solution. We apply Euler's criterion, and consider $a^{(p-1)/2} = 15^{(31-1)/2} = 15^{15}$ (mod 31). We have $15^2 = 225 \equiv 8 \pmod{31}$, $15^4 \equiv 8^2 \equiv 64 \equiv 2 \pmod{31}$, $15^8 \equiv 2^2 \equiv 4 \pmod{31}$, and $15^7 \equiv 15^4 \cdot 15^2 \cdot 15 \equiv 2 \cdot 8 \cdot 15 \equiv 240 \equiv 23 \pmod{31}$. So $15^{15} \equiv 15^8 \cdot 15^7 \equiv 4 \cdot 23 \equiv 92 \equiv -1 \pmod{31}$. Therefore, by Euler's criterion (Theorem 11.2), $x^2 \equiv 15 \pmod{31}$ $\boxed{\text{does not have a solution}}$. □

Note. Euler's criterion could be computationally involved for large numbers. We present an easier technique below. It is based on the notation we now introduce.

Definition. The *Legendre symbol*, $(a/p) = \left(\dfrac{a}{p}\right)$, where p is an odd prime and $p \nmid a$ is

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

Note. It would be easy to confuse the Legendre symbol with some type of division. We shall use context and verbiage to clarify the difference between Legendre symbols and regular division.

Exercise 11.8. What is $(4/5)$? $(4/7)$? $(4/p)$ for any odd prime p?

Solution. Since $2^2 \equiv 4 \pmod{5}$, then $(4/5) = \boxed{1}$. Since $2^2 \equiv 4 \pmod{7}$, then $(4/7) = \boxed{1}$. For $p = 3$, $1^1 \equiv 4 \pmod{3}$, so $(4/3) = \boxed{1}$. Since $2^2 \equiv 4 \pmod{p}$, for odd prime $p \geq 5$, then $(4/p) = \boxed{1}$ for such p. □

Note. To apply the Legendre symbol to large numbers, we use the following properties that allow us to simplify computations.

Theorem 11.3. The Legendre symbol has the properties

(A) if $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$,

(B) if $p \nmid a$, then $(a^2/p) = 1$, and

(C) if $p \nmid a$ and $p \nmid b$, then $(ab/p) = (a/p)(b/p)$.

Note. By considering the possible values of the Legendre symbol for a and b, we can paraphrase Theorem 11.3(C) as: 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.

Note. The historical comments in this note are based on the first few pages of Franz Lemmermeyer 's *Reciprocity Laws: From Euler to Eisenstein* (Springer Monographs in Mathematics), Springer (2000). Several pages of the book can be viewed on Google Books (accessed 3/12/2022); you might find several pages also available on the Amazon.com page for this book. The first to study the idea of reciprocity is French amateur mathematician Pierre de Fermat (August 17, 1601–January 12, 1665); this is maybe not surprising, given the prominent role of Fermat's "Little" Theorem (Theorem 6.1) in the proof of Euler's Criterion (Theorem 11.2). Fermat's interest in quadratic reciprocity arose in his study of numbers can be written as a sum of two squares (we explore this in Section 18. Sums of Two Squares; notice Lemma 18.4). He mentions this problem in a letter to Marin Mersenne (we mentioned correspondence between these two in Section 8. Perfect Numbers). Leonhard Euler (April 15, 1707–September 18, 1783) stated a claim equivalent to the Quadratic Reciprocity Theorem, but was unable to prove it in its entirety; his claim appeared in 1783 after his death in *Observationes circa divisionem quadratorum per numeros primes*, Opera Omnia **I - 3** (1783). Adrie-Marie Legendre (September 18, 1752–January 10, 1833) published a version of the Quadratic Reciprocity Theorem in 1788 by proving eight theorems for various values of two odd primes modulo 4 (in his *Recherches d'analyse indéterminée*, Histoire de l'Academie Royale des Sciences de Paris (1785), 465–559, Paris 1788). In 1789, Legendre introduces his "Legendre symbol" in *Essai sur la théorie des nombres*, 1st ed. Paris 1798. In this, he also proved "Legendre's Lemma": For each prime $a \equiv 1 \pmod{4}$, there exists prime $b \equiv 3 \pmod{4}$ such that the Legendre symbol $(1/b) = -1$. Carl F. Gauss (April 20, 1777–February 23, 1855) was the first to prove our modern version of the Quadratic Reciprocity Theorem. He published six proofs, and two more were found in his unpublished papers. He included a proof in his first 1801 edition of *Disquisitiones Arithmeticae* ["Investigations in Arithmetic"]. In this book, Gauss covers elementary number theory and some of, what today would be called, algebraic number theory. It is in this work that the congruence symbol, $\equiv$, is introduced. The seven sections of *Disquisitiones Arithmeticae* are: I. Congruent Numbers in General, II. Congruences of the First Degree, III. Residues of Powers, IV. Congruences of the Second Degree, V. Forms and Indeterminate Equations of the Second Degree, VI. Various Applications of the Preceding Discussions, and VII. Equations Defining Sections of a Circle. In fact, this book is still in print in English as: Carl Friedrich Gauss *Disquisitiones Arithmeticae*, English Edition, translated by Arthur A. Clarke (revised by William Waterhouse), NY: Springer-Verlag (1986) (originally Yale University Press, 1966).

Note. The Quadratic Reciprocity Theorem relates the Legendre symbols (p/q) and (q/p) for given odd primes p and q. Hence, it relates the solvability of quadratic congruences $x^2 \equiv p \pmod{q}$ and $x^2 \equiv q \pmod{p}$. It turns out to simply involve the values of p and q modulo 4. We now state the Quadratic Reciprocity Theorem and use it, but delay a proof until the next section.

Theorem 11.4. The Quadratic Reciprocity Theorem.

If p and q are odd primes and $p \equiv q \equiv 3 \pmod{4}$, then $(p/q) = -(q/p)$. Otherwise, $(p/q) = (q/p)$.

Note 11.A. Consider the quadratic congruence $x^2 \equiv 85 \pmod{97}$. To see if this has a solution, we just need to compute the Legendre symbol $(85/97)$. By Theorem 11.3(C), we have $(85/97) = ((17 \cdot 5)/97) = (17/97)(5/97)$. Now $97 \equiv 1 \pmod{4}$, so by the Quadratic Reciprocity Theorem (Theorem 11.4), $(17/97) = (97/17)$, and since $97 \equiv 12 \pmod{17}$ then by Theorem 11.3(A) $(97/17) = (12/17)$. So

$$\begin{aligned}
(12/17) &= ((4 \cdot 3)/17) = (4/17)(3/17) \text{ by Theorem 11.3(C)} \\
&= (3/17) \text{ by Theorem 11.3(B), since } 2^2 = 4 \text{ and so } (4/17) = 1 \\
&= (17/3) \text{ by Quadratic Reciprocity Theorem (Theorem 11.4)} \\
&= (2/3) \text{ by Theorem 11.3(A), because } 17 \equiv 2 \pmod{3} \\
&= -1 \text{ since } x^2 \equiv 2 \pmod{3} \text{ has no solution.}
\end{aligned}$$

For the other factor,

$$\begin{aligned}
(5/97) &= (97/5) \text{ by Quadratic Reciprocity Theorem (Theorem 11.4)} \\
&= (2/5) \text{ by Theorem 11.3(A), because } 97 \equiv 2 \pmod{5} \\
&= -1 \text{ since } x^2 \equiv 2 \pmod{5} \text{ has no solution.}
\end{aligned}$$

So $(85/97) = (17/97)(5/97) = (-1) \cdot (-1) = 1$ and, by the definition of Legendre symbol, the congruence $x^2 \equiv 85 \pmod{97}$ has a solution.

Theorem 11.5. If p is an odd prime, then

$$(-1/p) = 1 \text{ if } p \equiv 1 \pmod{4}, \text{ and } (-1/p) = -1 \text{ if } p \equiv 3 \pmod{4}.$$

Note. We can use Theorem 11.5 to compute (85/97) more directly than we did in Note 11.A. We have

$$\begin{aligned}
(85/97) &= (-12/97) \text{ by Theorem 11.3(A), because } -12 \equiv 85 \pmod{97} \\
&= (-1/97)(4/97)c(3/97) \text{ by Theorem 11.3(C)} \\
&= (-1/97)(3/97) \text{ by Theorem 11.3(B), since } 2^2 = 4 \text{ and so } (4/17) = 1 \\
&= (-1/97)(97/3) \text{ by Quadratic Reciprocity Theorem (Theorem 11.4)} \\
&= (-1/97)(1/3) \text{ by Theorem 11.3(A), because } 97 \equiv 1 \pmod{3} \\
&= (-1/97) \text{ since } x^2 \equiv 1 \pmod{3} \text{ has a solution and } (1/3) = 1 \\
&= 1 \text{ by Theorem 11.5, since } 97 \equiv 1 \text{ (mod4).}
\end{aligned}$$

Note. Notice that Theorem 11.5 says that we can find square roots of -1 modulo p when $p \equiv 1 \pmod{4}$. In fact, by Theorem 11.1 we know that under these conditions, there are two square roots of -1. The next result (which we prove in the next section) gives us conditions under which 2 has a square root.

Theorem 11.6. If p is an odd prime, then

$$(2/p) = 1 \text{ if } p \equiv 1 \text{ or } 7 \pmod{8}, \text{ and } (2/p) = -1 \text{ if } p \equiv 2 \text{ or } 5 \pmod{8}.$$

Note. Theorem 11.3, 11.4 (Quadratic Reciprocity Theorem), 11.5, and 11.6 allow us to evaluate any Legendre symbol. Theorems 11.3 and 11.4 let us "reduce" the symbols, and Theorems 11.5 and 11.6 allow us to evaluate the reduced symbols. For example, consider the Legendre symbol $(3201, 8191)$. First, since $3201 = 3{\cdot}11{\cdot}97$, so by Theorem 11.3(C) we have $(3201, 8191) = (3/8191)(11/8191)(97/8191)$. Next, by the Quadratic Reciprocity Theorem and Theorem 11.3(A) (since $8191 \equiv 1 \pmod 3$) we have: $(3, 8191) = -(8191/3) = -(1/3) = -(1) = -1$. Similarly, by the Quadratic Reciprocity Theorem, Theorem 11.3(A) (since $8191 \equiv 7 \pmod{11}$), the Quadratic Reciprocity Theorem (again), and Theorem 11.3(A) (again, this time since $11 \equiv 4 \pmod 7$), and Theorem 11.3(B) (which implies that $(4/7) = 1$) we have:

$$(11, 8191) = -(8191, 11) = -(7/11) = -(-(11/7)) = (11/7) = (4/7) = 1.$$

Finally, by the Quadratic Reciprocity Theorem, Theorem 11.3(A) (since $8191 \equiv 43 \pmod{97}$), the Quadratic Reciprocity Theorem (again), and Theorem 11.3(A) (again, this time since $97 \equiv 11 \pmod{43}$), the Quadratic Reciprocity Theorem (a third time), Theorem 11.3(A) (yet again, this time since $43 \equiv -1 \pmod{11}$), and Theorem 11.5 (which implies that $(-1/11) = -1$ since $11 \equiv 3 \pmod 4$) we have:

$$(97/8191) = (8191/97) = (43/97) = (97/43) = (11/43)$$
$$= -(43/11) = -(-1/11) = -(-1) = 1.$$

Therefore,

$$(3201, 8191) = (3/8191)(11/8191)(97/8191) = (-1)(1)(1) = -1.$$

There are Legendre symbol calculators online. For example, see EasyCalculation.com's Legendre symbol calculator webpage (notice that is shows some of the intermediate steps; accessed 3/13/2022).