Chapter 21

Is -1 a Square Modulo p? Is 2?

In the previous chapter we took various primes p and looked at the a's that were quadratic residues and the a's that were nonresidues. For example, we made a table of squares modulo 13 and used the table to see that 3 and 12 are QRs modulo 13, while 2 and 5 are NRs modulo 13.

In keeping with all of the best traditions of mathematics, we now turn this problem on its head. Rather than taking a particular prime p and listing the a's that are QRs and NRs, we instead fix an a and ask for which primes p is a a QR. To make it clear exactly what we're asking, we start with the particular value $a = -1$. The question that we want to answer is as follows:

For which primes p is -1 a QR?

We can rephrase this question in other ways, such as "For which primes p does the congruence $x^2 \equiv -1 \pmod{p}$ have a solution?" and "For which primes p is $\left(\frac{-1}{p}\right) = 1$?"

As always, we need some data before we can make any hypotheses. We can answer our question for small primes in the usual mindless way by making a table of $1^2, 2^2, 3^2, \ldots \pmod{p}$ and checking if any of the numbers are congruent to -1 modulo p. So, for example, -1 is not a square modulo 3, since $1^2 \not\equiv -1 \pmod{3}$ and $2^2 \not\equiv -1 \pmod{3}$, while -1 is a square modulo 5, since $2^2 \equiv -1 \pmod{5}$. Here's a more extensive list.

p	3	5	7	11	13	17	19	23	29	31
Solution(s) to $x^2 \equiv -1 \pmod{p}$	NR	$2, 3$	NR	NR	$5, 8$	$4, 13$	NR	NR	$12, 17$	NR

Reading from this table, we compile the following data:

$$-1 \text{ is a quadratic residue for } p = 5, 13, 17, 29.$$
$$-1 \text{ is a nonresidue for } p = 3, 7, 11, 19, 23, 31.$$

It's not hard to discern the pattern. If p is congruent to 1 modulo 4, then -1 seems to be a quadratic residue modulo p, and if p is congruent to 3 modulo 4, then -1 seems to be a nonresidue. We can express this guess using Legendre symbols,

$$\left(\frac{-1}{p}\right) \stackrel{?}{=} \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Let's check our conjecture on the next few cases. The next two primes, 37 and 41, are both congruent to 1 modulo 4 and, sure enough,

$$x^2 \equiv -1 \pmod{37} \text{ has the solutions } x \equiv 6 \text{ and } 31 \pmod{37}, \text{ and}$$
$$x^2 \equiv -1 \pmod{41} \text{ has the solutions } x \equiv 9 \text{ and } 32 \pmod{41}.$$

Similarly, the next two primes 43 and 47 are congruent to 3 modulo 4, and we check that -1 is a nonresidue for 43 and 47. Our guess is looking good!

The tool that we use to verify our conjecture might be called the "Square Root of Fermat's Little Theorem." How, you may well ask, does one take the square root of a theorem? Recall that Fermat's Little Theorem (Chapter 9) says

$$a^{p-1} \equiv 1 \pmod p.$$

We won't really be taking the square root of this theorem, of course. Instead, we take the square root of the quantity a^{p-1} and ask for its value. So we want to answer the following question:

Let $A = a^{(p-1)/2}$. What is the value of A modulo p?

One thing is obvious. If we square A, then Fermat's Little Theorem tells us that

$$A^2 = a^{p-1} \equiv 1 \pmod p.$$

Hence, p divides $A^2 - 1 = (A-1)(A+1)$, so either p divides $A-1$ or p divides $A+1$. (Notice how we are using Lemma 7.1, which is the property of prime numbers that we proved on page 46.) Thus A must be congruent to either $+1$ or -1.

Here are a few random values of p, a, and A. For comparison purposes, we have also included the value of the Legendre symbol $\left(\frac{a}{p}\right)$. Do you see a pattern?

p	11	31	47	97	173	409	499	601	941	1223
a	3	7	10	15	33	78	33	57	222	129
$A \pmod p$	1	1	-1	-1	1	-1	1	-1	1	1
$\left(\frac{a}{p}\right)$	1	1	-1	-1	1	-1	1	-1	1	1

It certainly appears that $A \equiv 1 \pmod p$ when a is a quadratic residue and that $A \equiv -1 \pmod p$ when a is a nonresidue. In other words, it looks like $A \pmod p$ has the same value as the Legendre symbol $\left(\frac{a}{p}\right)$. We use a counting argument to verify this assertion, which goes by the name of Euler's Criterion. [For an alternative proof of this important result, see Exercise 28.8(c).]

Theorem 21.1 (Euler's Criterion)**.** *Let p be an odd prime. Then*

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

Proof. Suppose first that a is a quadratic residue, say $a \equiv b^2 \pmod p$. Then Fermat's Little Theorem (Theorem 9.1) tells us that

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

Hence $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p$, which is Euler's Criterion when a is a quadratic residue.

We next consider the congruence

$$X^{(p-1)/2} - 1 \equiv 0 \pmod p.$$

We have just proven that every quadratic residue is a solution to this congruence, and we know from Theorem 20.1 that there are exactly $\frac{1}{2}(p-1)$ distinct quadratic residues. We also know from the Polynomial Roots Mod p Theorem (Theorem 8.2 on page 60) that this polynomial congruence can have at most $\frac{1}{2}(p-1)$ distinct solutions. Hence

$$\big\{\text{solutions to } X^{(p-1)/2} - 1 \equiv 0 \pmod p\big\} = \big\{\text{quadratic residues modulo } p\big\}.$$

Now let a be a nonresidue. Fermat's Little Theorem tells us that $a^{p-1} \equiv 1 \pmod p$, so

$$0 \equiv a^{p-1} - 1 \equiv (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \pmod p.$$

The first factor is not zero modulo p, because we already showed that the solutions to $X^{(p-1)/2} - 1 \equiv 0 \pmod{p}$ are the quadratic residues. Hence the second factor must vanish modulo p, so

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

This shows that Euler's Criterion is also true for nonresidues. □

Using Euler's Criterion, it is very easy to determine if -1 is a quadratic residue modulo p. For example, if we want to know whether -1 is a square modulo the prime $p = 6911$, we just need to compute

$$(-1)^{(6911-1)/2} = (-1)^{3455} = -1.$$

Euler's Criterion then tells us that

$$\left(\frac{-1}{6911}\right) \equiv -1 \pmod{6911}.$$

But $\left(\frac{a}{p}\right)$ is always either $+1$ or -1, so in this case we must have $\left(\frac{-1}{6911}\right) = -1$. Hence, -1 is a nonresidue modulo 6911.

Similarly, for the prime $p = 7817$ we find that

$$(-1)^{(7817-1)/2} = (-1)^{3908} = 1.$$

Hence, $\left(\frac{-1}{7817}\right) = 1$, so -1 is a quadratic residue modulo 7817. Observe that, although we now know that the congruence

$$x^2 \equiv -1 \pmod{7817}$$

has a solution, we still don't have any efficient way to find a solution. The solutions turn out to be $x \equiv 2564 \pmod{7817}$ and $x \equiv 5253 \pmod{7817}$.

As these two examples make clear, Euler's Criterion can be used to determine exactly which primes have -1 as a quadratic residue. This elegant result, which answers the initial question in the title of this chapter, is the first part of the Law of Quadratic Reciprocity.

Theorem 21.2 (Quadratic Reciprocity)**.** (Part I) *Let p be an odd prime. Then*

$$\begin{aligned} -1 \textit{ is a quadratic residue modulo } p \quad &\textit{if } p \equiv 1 \pmod{4}, \textit{ and} \\ -1 \textit{ is a nonresidue modulo } p \quad &\textit{if } p \equiv 3 \pmod{4}. \end{aligned}$$

In other words, using the Legendre symbol,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod{4}, \\ -1 & \textit{if } p \equiv 3 \pmod{4}. \end{cases}$$

Proof. Euler's Criterion says that

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

Suppose first that $p \equiv 1 \pmod{4}$, say $p = 4k+1$. Then

$$(-1)^{(p-1)/2} = (-1)^{2k} = 1, \quad \text{so} \quad 1 \equiv \left(\frac{-1}{p}\right) \pmod{p}.$$

But $\left(\frac{-1}{p}\right)$ is either $+1$ or -1, so it must equal 1. This proves that if $p \equiv 1 \pmod{4}$ then $\left(\frac{-1}{p}\right) = 1$.

Next we suppose that $p \equiv 3 \pmod{4}$, say $p = 4k+3$. Then

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1, \quad \text{so} \quad -1 \equiv \left(\frac{-1}{p}\right) \pmod{p}.$$

This shows that $\left(\frac{-1}{p}\right)$ must equal -1, which completes the proof of Quadratic Reciprocity (Part I). □

We can use the first part of Quadratic Reciprocity to answer a question left over from Chapter 12. As you may recall, we showed that there are infinitely many primes that are congruent to 3 modulo 4, but we left unanswered the analogous question for primes congruent to 1 modulo 4.

Theorem 21.3 (Primes 1 (Mod 4) Theorem)**.** *There are infinitely many primes that are congruent to 1 modulo 4.*

Proof. Suppose we are given a list of primes $p_1, p_2, \ldots, p_r$, all of which are congruent to 1 modulo 4. We are going to find a new prime, not in our list, that is congruent to 1 modulo 4. Repeating this process gives a list of any desired length.

Consider the number

$$A = (2p_1p_2 \cdots p_r)^2 + 1.$$

We know that A can be factored into a product of primes, say

$$A = q_1q_2 \cdots q_s.$$

It is clear that $q_1, q_2, \ldots, q_s$ are not in our original list, since none of the p_i's divide A. So all we need to do is show that at least one of the q_i's is congruent to 1 modulo 4. In fact, we'll see that all of them are.

First we note that A is odd, so all the q_i's are odd. Next, each q_i divides A, so

$$(2p_1p_2\cdots p_r)^2 + 1 = A \equiv 0 \pmod{q_i}.$$

This means that $x = 2p_1p_2\cdots p_r$ is a solution to the congruence

$$x^2 \equiv -1 \pmod{q_i},$$

so -1 is a quadratic residue modulo q_i. Now Quadratic Reciprocity tells us that $q_i \equiv 1 \pmod 4$. □

We can use the procedure described in this proof to produce a list of primes that are congruent to 1 modulo 4. Thus, if we start with $p_1 = 5$, then we form $A = (2p_1)^2 + 1 = 101$, so our second prime is $p_2 = 101$. Then

$$A = (2p_1p_2)^2 + 1 = 1020101,$$

which is again prime, so our third prime is $p_3 = 1020101$. We'll go one more step,

$$\begin{aligned} A &= (2p_1p_2p_3)^2 + 1 \\ &= 1061522231810040101 \\ &= 53 \cdot 1613 \cdot 12417062216309. \end{aligned}$$

Notice that all the primes 53, 1613, and 12417062216309 are congruent to 1 modulo 4, just as predicted by the theory.

Having successfully answered the first question in the title of this chapter, we move on to the second question and consider $a = 2$, the "oddest" of all primes. Just as we did with $a = -1$, we are looking for some simple characterization for the primes p such that 2 is a quadratic residue modulo p. Can you find the pattern in the following data, where the line labeled $x^2 \equiv 2$ gives the solutions to $x^2 \equiv 2 \pmod p$ if 2 is a quadratic residue modulo p and is marked NR if 2 is a nonresidue?

p	3	5	7	11	13	17	19	23	29	31
$x^2 \equiv 2$	NR	NR	3, 4	NR	NR	6, 11	NR	5, 18	NR	8, 23

p	37	41	43	47	53	59	61	67	71	73
$x^2 \equiv 2$	NR	17, 24	NR	7, 40	NR	NR	NR	NR	12, 59	32, 41

p	79	83	89	97	101	103	107	109	113	127
$x^2 \equiv 2$	9, 70	NR	25, 64	14, 83	NR	38, 65	NR	NR	51, 62	16, 111

Here's the list of primes separated according to whether 2 is a residue or a nonresidue.

$$\begin{aligned} 2 \text{ is a quadratic residue for } p = {} & 7, 17, 23, 31, 41, 47, 71, 73, \\ & 79, 89, 97, 103, 113, 127 \\ 2 \text{ is a nonresidue for } p = {} & 3, 5, 11, 13, 19, 29, 37, 43, 53, 59, \\ & 61, 67, 83, 101, 107, 109 \end{aligned}$$

For $a = -1$, it turned out that the congruence class of p modulo 4 was crucial. Is there a similar pattern if we reduce these two lists of primes modulo 4? Here's what happens if we do.

$$\begin{aligned} &7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, 103, 113, 127 \\ &\qquad \equiv 3, 1, 3, 3, 1, 3, 3, 1, 3, 1, 1, 3, 1, 3 \pmod 4, \\ &3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83, 101, 107, 109 \\ &\qquad \equiv 3, 1, 3, 1, 3, 1, 1, 3, 1, 3, 1, 3, 3, 1, 3, 1 \pmod 4. \end{aligned}$$

This doesn't look too promising. Maybe we should try reducing modulo 3.

$$\begin{aligned} &7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, 103, 113, 127 \\ &\qquad \equiv 1, 2, 2, 1, 2, 2, 2, 1, 1, 2, 1, 1, 2, 1 \pmod 3 \\ &3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83, 101, 107, 109 \\ &\qquad \equiv 0, 2, 2, 1, 1, 2, 1, 1, 2, 2, 1, 1, 2, 2, 2, 1 \pmod 3. \end{aligned}$$

This doesn't look any better. Let's make one more attempt before we give up. What happens if we reduce modulo 8?

$$\begin{aligned} &7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, 103, 113, 127 \\ &\qquad \equiv 7, 1, 7, 7, 1, 7, 7, 1, 7, 1, 1, 7, 1, 7 \pmod 8 \\ &3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83, 101, 107, 109 \\ &\qquad \equiv 3, 5, 3, 5, 3, 5, 5, 3, 5, 3, 5, 3, 3, 5, 3, 5 \pmod 8. \end{aligned}$$

Eureka! It surely can't be a coincidence that the first line is all 1's and 7's and the second line is all 3's and 5's. This suggests the general rule that 2 is a quadratic residue modulo p if p is congruent to 1 or 7 modulo 8 and that 2 is a nonresidue if p is congruent to 3 or 5 modulo 8. In terms of Legendre symbols, we would write

$$\left(\frac{2}{p}\right) \stackrel{?}{=} \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

Can we use Euler's Criterion to verify our guess? Unfortunately, the answer is no, or at least not in any obvious way, since there doesn't seem to be an easy method to calculate $2^{(p-1)/2} \pmod{p}$. However, if you go back and examine our proof of Fermat's Little Theorem in Chapter 9, you'll see that we took the numbers $1, 2, \ldots, p-1$, multiplied each one by a, and then multiplied them all together. This gave us a factor of a^{p-1} to pull out. In order to use Euler's Criterion, we only want $\frac{1}{2}(p-1)$ factors of a to pull out, so rather than starting with all of the numbers from 1 to p, we just take the numbers from 1 to $\frac{1}{2}(p-1)$. We illustrate this idea, which is due to Gauss, to determine if 2 is a quadratic residue modulo 13.

We begin with half the numbers from 1 to 12: $1, 2, 3, 4, 5, 6$. If we multiply each by 2 and then multiply them together, we get

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 &= (2 \cdot 1)(2 \cdot 2)(2 \cdot 3)(2 \cdot 4)(2 \cdot 5)(2 \cdot 6) \\ &= 2^6 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \\ &= 2^6 \cdot 6!. \end{aligned}$$

Notice the factor of $2^6 = 2^{(13-1)/2}$, which is the number we're really interested in.

Gauss's idea is to take the numbers $2, 4, 6, 8, 10, 12$ and reduce each of them modulo 13 to get a number lying between -6 and 6. The first three stay the same, but we need to subtract 13 from the last three to get them into this range. Thus,

$$\begin{array}{lll} 2 \equiv 2 \pmod{13} & 4 \equiv 4 \pmod{13} & 6 \equiv 6 \pmod{13} \\ 8 \equiv -5 \pmod{13} & 10 \equiv -3 \pmod{13} & 12 \equiv -1 \pmod{13}. \end{array}$$

Multiplying these numbers together, we find that

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 &\equiv 2 \cdot 4 \cdot 6 \cdot (-5) \cdot (-3) \cdot (-1) \\ &\equiv (-1)^3 \cdot 2 \cdot 4 \cdot 6 \cdot 5 \cdot 3 \cdot 1 \\ &\equiv -6! \pmod{13}. \end{aligned}$$

Equating these two values of $2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \pmod{13}$, we see that

$$2^6 \cdot 6! \equiv -6! \pmod{13}.$$

This implies that $2^6 \equiv -1 \pmod{13}$, so Euler's Criterion tells us that 2 is a non-residue modulo 13.

Let's briefly use the same ideas to check if 2 is a quadratic residue modulo 17. We take the numbers from 1 to 8, multiply each by 2, multiply them together, and calculate the product in two different ways. The first way gives

$$2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \cdot 14 \cdot 16 = 2^8 \cdot 8!.$$

For the second way, we reduce modulo 17 to bring the numbers into the range from -8 to 8. Thus,

$$\begin{array}{lll} 2 \equiv 2 \pmod{17} & 4 \equiv 4 \pmod{17} & 6 \equiv 6 \pmod{17} \\ 8 \equiv 8 \pmod{17} & 10 \equiv -7 \pmod{17} & 12 \equiv -5 \pmod{17} \\ 14 \equiv -3 \pmod{17} & 16 \equiv -1 \pmod{17}. & \end{array}$$

Multiplying these together gives

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \cdot 14 \cdot 16 &\equiv 2 \cdot 4 \cdot 6 \cdot 8 \cdot (-7) \cdot (-5) \cdot (-3) \cdot (-1) \\ &\equiv (-1)^4 \cdot 8! \pmod{17}. \end{aligned}$$

Therefore, $2^8 \cdot 8! \equiv (-1)^4 \cdot 8! \pmod{17}$, so $2^8 \equiv 1 \pmod{17}$, and hence 2 is a quadratic residue modulo 17.

Now let's think about Gauss's method a little more generally. Let p be any odd prime. To make our formulas simpler, we let

$$P = \frac{p-1}{2}.$$

We start with the even numbers $2, 4, 6, \ldots, p-1$. Multiplying them together and factoring out a 2 from each number gives

$$2 \cdot 4 \cdot 6 \cdots (p-1) = 2^{(p-1)/2} \cdot 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} = 2^P \cdot P!.$$

The next step is to take the list $2, 4, 6, \ldots, p-1$ and reduce each number modulo p so that it lies in the range from $-P$ to P, that is, between $-(p-1)/2$ and $(p-1)/2$. The first few numbers won't change, but at some point in the list we'll start hitting numbers that are larger than $(p-1)/2$, and each of these large numbers needs to have p subtracted from it. Notice that the number of minus signs introduced is exactly the number of times we need to subtract p. In other words,

$$\text{Number of minus signs} = \begin{pmatrix} \text{Number of integers in the list} \\ 2, 4, 6, \ldots, (p-1) \\ \text{that are larger than } \frac{1}{2}(p-1) \end{pmatrix}.$$

The following illustration may help to explain this procedure.

$$\underbrace{2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \cdots}_{\substack{\text{Numbers } \le (p-1)/2 \\ \text{are left unchanged.}}} \Big| \underbrace{\cdots (p-5) \cdot (p-3) \cdot (p-1)}_{\substack{\text{Numbers } > (p-1)/2. \\ \text{Need to subtract } p \text{ from each.}}}$$

Comparing the two products, we get

$$2^P \cdot P! = 2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{(\text{number of minus signs})} \cdot P! \pmod{p},$$

so canceling $P!$ from each side gives the fundamental formula

$$2^{(p-1)/2} \equiv (-1)^{(\text{number of minus signs})} \pmod{p}.$$

Using this formula, it is easy to verify our earlier guess, thereby answering the second question in the chapter title.

Theorem 21.4 (Quadratic Reciprocity)**.** (Part II) *Let p be an odd prime. Then 2 is a quadratic residue modulo p if p is congruent to 1 or 7 modulo 8, and 2 is a nonresidue modulo p if p is congruent to 3 or 5 modulo 8. In terms of the Legendre symbol,*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8}. \end{cases}$$

Proof. There are actually four cases to consider, depending on the value of p modulo 8. We do two of them and leave the other two for you to do.

We start with the case that $p \equiv 3 \pmod{8}$, say $p = 8k+3$. We need to list the numbers $2, 4, \ldots, p-1$ and determine how many of them are larger than $\frac{1}{2}(p-1)$. In this case, $p-1 = 8k+2$ and $\frac{1}{2}(p-1) = 4k+1$, so the cutoff is as indicated in the following diagram:

$$2 \cdot 4 \cdot 6 \cdots 4k \quad \Big| \quad (4k+2) \cdot (4k+4) \cdots (8k+2).$$

We need to count how many numbers there are to the right of the vertical bar. In other words, how many even numbers are there between $4k+2$ and $8k+2$? The answer is $2k+1$. (If this isn't clear to you, try a few values for k and you'll see why it's correct.) This shows that there are $2k+1$ minus signs, so the fundamental formula given above tells us that

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

Now Euler's Criterion says that 2 is a nonresidue, so we have proved that 2 is a nonresidue for any prime p that is congruent to 3 modulo 8.

Next let's look at the primes that are congruent to 7 modulo 8, say $p = 8k+7$. Now the even numbers $2, 4, \ldots, p-1$ are the numbers from 2 to $8k+6$, and the midpoint is $\frac{1}{2}(p-1) = 4k+3$. The cutoff in this case is

$$2 \cdot 4 \cdot 6 \cdots (4k+2) \quad \Big| \quad (4k+4) \cdot (4k+6) \cdots (8k+6).$$

There are exactly $2k+2$ numbers to the right of the vertical bar, so we get $2k+2$ minus signs. This yields

$$2^{(p-1)/2} \equiv (-1)^{2k+2} \equiv 1 \pmod{p},$$

so Euler's Criterion tells us that 2 is a quadratic residue. This proves that 2 is a quadratic residue for any prime p that is congruent to 7 modulo 8. □

Exercises

21.1. Determine whether each of the following congruences has a solution. (All of the moduli are primes.)

(a) $x^2 \equiv -1 \pmod{5987}$
(b) $x^2 \equiv 6780 \pmod{6781}$
(c) $x^2 + 14x - 35 \equiv 0 \pmod{337}$
(d) $x^2 - 64x + 943 \equiv 0 \pmod{3011}$

[*Hint*. For (c), use the quadratic formula to find out what number you need to take the square root of modulo 337, and similarly for (d).]

21.2. Use the procedure described in the Primes 1 (Mod 4) Theorem to generate a list of primes congruent to 1 modulo 4, starting with the seed $p_1 = 17$.

21.3. Here is a list of the first few primes for which 3 is a quadratic residue and a nonresidue.

$$\begin{aligned} \text{Quadratic Residue:} &\quad p = 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107, 109 \\ \text{Nonresidue:} &\quad p = 5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89, 101, 103, 113, 127 \end{aligned}$$

Try reducing this list modulo m for various m's until you find a pattern, and make a conjecture explaining which primes have 3 as a quadratic residue.

21.4. Finish the proof of Quadratic Reciprocity (Part II) for the other two cases: primes congruent to 1 modulo 8 and primes congruent to 5 modulo 8.

21.5. Use the same ideas we used to verify Quadratic Reciprocity (Part II) to verify the following two assertions.

(a) If p is congruent to 1 modulo 5, then 5 is a quadratic residue modulo p.
(b) If p is congruent to 2 modulo 5, then 5 is a nonresidue modulo p.

[*Hint*. Reduce the numbers $5, 10, 15, \ldots, \frac{5}{2}(p-1)$ so that they lie in the range from $-\frac{1}{2}(p-1)$ to $\frac{1}{2}(p-1)$ and check how many of them are negative.]

21.6. In Exercise 20.2 we defined A and B to be the sums of the residues, respectively nonresidues, modulo p. Part (d) of that exercise asked you to find a condition on p which implies that $A = B$. Using the material in this section, prove that your criterion is correct. [*Hint*. The important fact you'll need is the condition for -1 to be a quadratic residue.]