1 Exercises

1.1

Convert $2x^2 + 3x + 1 \equiv 0 \pmod 5$ to a quadratic congruence whose first coefficient is 1.

Since $3 * 2 \equiv 1 \pmod 5$, the congruence is equivalent to $x^2 + 4x + 3 \equiv 0 \pmod 5$.

1.2

Change the quadratic in Exercise 1 to the form (3).

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

1.3

By inspection, find all the solutions of the congruence in Exercise 2.

$y^2 \equiv 1 \pmod 5$ has solutions 1 and 4, so the congruence in Exercise 2 has solutions 2 and 4.

1.4

If $p > 3$, what are the two solutions of $x^2 \equiv 4 \pmod p$?

2 and $p - 2$.

1.5

For what values of a does $x^2 \equiv a \pmod 7$ have two solutions?

1, 4, 2.

1.6

Find the solutions of $x^2 \equiv 8 \pmod{31}$.

$8 \equiv 39 \equiv 70 \equiv 101 \equiv 132 \equiv 2^2 * 33 \equiv 2^2 * 2 \pmod{31}$.
$2 \equiv 33 \equiv 64 \equiv 8^2 \pmod{31}$.
$2^2 * 8^2 \equiv 16^2 \pmod{31}$.
15 and 16 are solutions to $x^2 \equiv 8 \pmod{31}$.

1.7

What is (1/3)? (1/7)? (1/11)? In general, what is $(1/p)$?

All of them must be 1, since 1 and $p - 1$ are solutions to the congruences.

1.8

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

For $p > 3$, it should be 1, as 2, $p - 2$ are both solutions.

1.9

Induce a theorem from the two preceding exercises.

$(k^2/p) = 1$ as long as $p \nmid k$.

1.10

Verify that if $(a/p) = -1$ and $a \equiv b \pmod p$, then $(b/p) = -1$.

If $(a/p) = -1$, then $\nexists x \ni x^2 \equiv a \equiv b \pmod p$.

1.11

Prove (B), using (6).

$(a^2/p) \equiv a^{2(p-1)/2} \equiv a^{p-1}$. By Fermat's Theorem, $a^{p-1} \equiv 1 \pmod p$. So, $(a^2/p) \equiv 1 \pmod p$, and since $(a^2/p) = 1$ or -1, $(a^2/p) = 1$.

1.12

Prove that $(4a/p) = (a/p)$.

Know that $(4a/p) = (4/p)(a/p)$. Also know that $p \nmid 4$, as p is an odd prime. So we can use the result from the previous, that $(2^2/p) = 1$.

1.13

Evaluate $(19/5)$ and $(-9/13)$ by using (A) and (B).

$(19/5) = (4/5) = (2^2/5) = 1$. $(-9/13) = (4/13) = (2^2/13) = 1$.

1.14

For which of the primes 3, 5, 7, 11, 13, 17, 19, and 23 is -1 a quadratic residue?

-1 is a quadratic residue for 5, 13, and 17.

1.15

Evaluate $(6/7)$ and $(2/23)(11/23)$.

$(6/7) = (-1/7) = -1$. $(2/23)(11/23) = (23/2) * -(23/11) = -(1/2)(1/11) = -1$.

2 Problems

2.1

Which of the following congruences have solutions?

$$x^2 \equiv 7 \pmod{53}, \quad x^2 \equiv 14 \pmod{31}, \quad x^2 \equiv 53 \pmod 7, \quad x^2 \equiv 25 \pmod{997}.$$

$(7/53) = (53/7) = (4/7) = 1$.
$(14/31) = (2/31)(7/31) = -(31/2)(31/7) = -(1/2)(3/7) = 1$.
$(53/7) = (4/7) = 1$.
$(25/997) = 1$.

2.2

Which of the following congruences have solutions?

$$x^2 \equiv 8 \pmod{53}, \quad x^2 \equiv 15 \pmod{31}, \quad x^2 \equiv 54 \pmod 7, \quad x^2 \equiv 625 \pmod{9973}.$$

$(8/53) = (2/53)(4/53) = (2/53) = -1$.
$(15/31) = (3/31)(5/31) = -(31/3)(31/5) = -(1/3)(1/5) = -1$.

$(54/7) = (5/7) = -1$.
$(625/9973) = (25/9973)(25/9973) = 1$.

2.3

Find solutions for the congruences in Problem 1 that have them.

$x^2 \equiv 7 \equiv 60 \equiv 2^2 * 15 \pmod{53}$.
$15 \equiv 68 \equiv 121 \equiv 11^2 \pmod{53}$.
So, 22 and 31 are solutions to the congruence.
$x^2 \equiv 14 \equiv 169 \equiv 13^2 \pmod{31}$.
So, 13 and 18 are solutions to the congruence.
$x^2 \equiv 53 \equiv 4 \equiv 2^2 \pmod 7$.
So, 2 and 5 are solutions to the congruence.
$x^2 \equiv 25 \pmod{997}$.
5 and 992 are solutions to the congruence.

2.4

Find solutions for the congruences in Problem 2 that have them.

$x^2 \equiv 625 \pmod{9973}$.
25 and 9948 are solutions to the congruence.

2.5

Calculate (33/71), (34/71), (35/71), and (36/71).

$(33/71) = (71/33) = (5/33) = (33/5) = (3/5) = -1$.
$(33/71) = (2/71)(17/71) = (71/17) = (3/17) = (17/3) = (2/3) = -1$.
$(35/71) = (5/71)(7/71) = -(71/5)(71/7) = -(1/5)(1/7) = -1$.
$(36/71) = 1$.

2.6

Calculate (33/73), (34/73), (35/73), and (36/73).

$(33/73) = (3/73)(11/73) = (73/3)(73/11) = (1/3)(7/11) = -(11/7) = -(4/7) = -1$.
$(34/73) = (2/73)(17/73) = (73/17) = (5/17) = (17/5) = (2/5) = -1$.
$(35/73) = (5/73)(7/73) = (3/5)(3/7) = -(2/3)(1/3) = 1$.
$(36/73) = 1$.

2.7

Solve $2x^2 + 3x + 1 \equiv 0 \pmod 7$ and $2x^2 + 3x + 1 \equiv 0 \pmod{101}$.

$$x^2 + 12x + 4 \equiv 0 \pmod 7$$
$$(x+6)^2 \equiv 4 \pmod 7$$
$$x \in \{3, 6\},$$
$$x^2 + 52x + 51 \equiv 0 \pmod{101},$$
$$(x+26)^2 \equiv 625 \pmod{101},$$
$$x \in \{50, 100\}$$

2.8

Solve $3x^2 + x + 8 \equiv 0 \pmod{11}$ and $3x^2 + x + 52 \equiv 0 \pmod{11}$.

$$\begin{gathered}
x^2 + 4x + 10 \equiv 0 \pmod{11} \\
(x+2)^2 \equiv 16 \pmod{11} \\
x \in \{2, 5\}, \\
x^2 + 4x + 10 \equiv 0 \pmod{11} \\
x \in \{2, 5\}
\end{gathered}$$

2.9

Calculate $(1234/4567)$ and $(4321/4567)$.

$$\begin{gathered}
(1234/4567) = (2/4567)(617/4567) = (4567/617) = (248/617) \\
= (2/617)(4/617)(31/617) = (31/617) = (617/31) = (28/31) \\
= (4/31)(7/31) = -(31/7) = -(3/7) = 1 \\
(4321/4567) = (29/4567)(149/4567) = (4567/29)(4567/149) \\
= (14/29)(97/149) = (2/29)(7/29)(149/97) = -(29/7)(52/97) \\
= -(1/7)(4/97)(13/97) = -(97/13) = -(6/13) = 1
\end{gathered}$$

2.10

Calculate $(1356/4567)$ and $(6531/4567)$.

$$\begin{gathered}
(1356/4567) = (3/4567)(4/4567)(113/4567) = -(4567/3)(4567/113) \\
= -(1/3)(47/113) = -(113/47) = -(19/47) = (47/19) = (9/19) = 1 \\
(6531/4567) = (3/4567)(7/4567)(311/4567) = -(3/7)(213/311) \\
= (3/311)(71/311) = (2/3)(27/71) = -(3/71) = (2/3) = -1
\end{gathered}$$

2.11

Show that if $p = q + 4a$ (p and q are odd primes), then $(p/q) = (a/q)$.

Know $p \equiv 4a \pmod{q}$, so $(p/q) = (4a/q) = (4/q)(a/q) = (a/q)$.

2.12

Show that if $p = 12k + 1$ for some k, then $(3/p) = 1$.

Know $p \equiv 1 \pmod 3$, so $(p/3) = (1/3) = 1$. Since $p \equiv 1 \pmod 4$, know that $(p/3) = (3/p)$, so $(3/p) = 1$.

2.13

Show that Theorem 6 could also be written $(2/p) = (-1)^{(p^2-1)/8}$ for odd primes p.

If $p \equiv r \pmod 8$, then $p = 8k + r$, $p^2 = 64k^2 + 16k + r^2$. The first two terms divided by 8 are $8k^2 + 2k$, which is always even. So we only have to examine $(r^2 - 1)/8 \pmod 2$ for the following. If $p \equiv 1 \pmod 8$, then $(1-1)/8 \equiv 0 \pmod 2$. If $p \equiv 7 \pmod 8$, then $(49-1)/8 \equiv 0 \pmod 2$. Since -1 to an even power is 1, and $(2/p) = 1$ if $p \equiv 1$ or $7 \pmod 8$, the equation holds for $p \ni (2/p) = 1$. If $p \equiv 3 \pmod 8$, then $(9-1)/8 \equiv 1 \pmod 2$. If $p \equiv 5 \pmod 8$, then $(25-1)/8 \equiv 1 \pmod 2$. Since -1 to an odd power is -1, and $(2/p) = -1$ if $p \equiv 3$ or $5 \pmod 8$, the equation holds for $p \ni (2/p) = -1$.

2.14

Show that the quadratic reciprocity theorem could also be written $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$ for odd primes p and q.

The quadratic reciprocity theorem states that if $p \equiv q \equiv 3 \pmod 4$, then $(p/q) = -(q/p)$. Otherwise, $(p/q) = (q/p)$. Since p, q are odd primes, each can either be $\equiv 1$ or $\equiv 3 \pmod 4$. If both $p, q \equiv 3 \pmod 4$, then $(4k_p + 2)(4k_q + 2)/4 = (16k_pk_1 + 8k_p + 8k_q + 4)/4$. Thus the exponent is odd, and -1 raised to that exponent is -1. We also know that if $p \equiv q \equiv 3 \pmod 4$, then $(p/q) = -(q/p)$, so $(p/q)(q/p) = -((q/p)^2) = -1$. Now consider both $p, q \equiv 1 \pmod 4$. Then $(p-1)(q-1)/4 = 4k_p4k_q/4$ for some k_p, k_q, and the exponent is even. Without loss of generality, if $p \equiv 1$ and $q \equiv 3 \pmod 4$, then $(p-1)(q-1)/4 = 4k_p(4k_q + 2)/4$, and the exponent is even. If the exponent is even, then -1 raised to that exponent is 1. We know that if either p or $q \not\equiv 3 \pmod 4$, then $(p/q) = (q/p)$, so $(p/q)(q/p) = (q/p)^2 = 1$.

2.15

Student A says, "I've checked all the way up to 100 and I still haven't found n so that n^2+1 is divisible by 7. I'm tired now - I'll find one tomorrow." Student B says, after a few seconds of reflection, "No you won't." How did B know so quickly?

This problem can be rewritten as $x^2 \equiv 6 \pmod 7$. Can examine the first few integers (under 7) to see that 6 is a nonresidue $\pmod 7$: $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 2 \pmod 7$.

2.16

Show that if a is a quadratic residue $\pmod p$ and $ab \equiv 1 \pmod p$, then b is a quadratic residue $\pmod p$.

It follows that $(a/p) = 1$. We know that $(1/p) = 1$ for any p. So, since $ab \equiv 1 \pmod p$, $(ab/p) = (1/p) = 1$. Also know that $p \nmid a, b$, since if it did divide either, $ab \equiv 0 \pmod p$. Then $(ab/p) = (a/p)(b/p)$, and $(b/p) = 1$.

2.17

Does $x^2 \equiv 211 \pmod{159}$ have a solution? Note that 159 is not prime.

Yes, by inspection $211 + 2 * 159 = 529 = 23^2$ is a solution.

2.18

Prove that if $p \equiv 3 \pmod 8$ and $(p-1)/2$ is prime, then $(p-1)/2$ is a quadratic residue $\pmod p$.

Since $\frac{p-1}{2}$ is prime, we can use the quadratic reciprocity theorem. If $p \equiv 3 \pmod 8$, then $p \equiv 3 \pmod 4$. But, if we write $p = 8k + 3$, we see that $\frac{p-1}{2} = \frac{8k+3-1}{2} = 4k + 1 \equiv 1 \pmod 4$. So, $(\frac{p-1}{2}/p) = (p/\frac{p-1}{2})$. $p \equiv p - 2(\frac{p-1}{2}) \equiv 1 \pmod{\frac{p-1}{2}}$, so $(p/\frac{p-1}{2}) = (1/\frac{p-1}{2}) = 1$.

2.19

Generalize Problem 16 by finding what condition on r will guarantee that if a is a quadratic residue $\pmod p$ and $ab \equiv r \pmod p$, then b is a quadratic residue $\pmod p$.

It follows that $(a/p) = 1$. Since $ab \equiv r \pmod p$, $(ab/p) = (r/p)$. Since $p \nmid a, b$, $(ab/p) = (a/p)(b/p) = (b/p) = (r/p)$. So, b a quadratic residue if, and only if, r a quadratic residue.

2.20

Suppose that $p = q + 4a$, where p and q are odd primes. Show that $(a/p) = (a/q)$.

Know that $p \equiv 4a \pmod{q}$, so $(p/q) = (4a/q) = (a/q)$. Conversely, $q \equiv -4a \pmod{p}$, so $(q/p) = (-1/p)(4a/p) = (-1/p)(a/p)$. Know that if $p \equiv 1 \pmod{4}$, then $(-1/p) = 1$. Observe also that $p \equiv q \pmod{4}$, so if $p \equiv 1 \pmod{4}$, then $(q/p) = (p/q)$. So, if $p \equiv 1 \pmod{4}$, then $(p/q) = (a/p)$, and $(a/p) = (a/q)$. If $p \equiv 3 \pmod{4}$, then $(-1/p) = -1$ and $(q/p) = -(p/q)$. So then $-(p/q) = -(a/p)$, or $(p/q) = (a/p)$, and $(a/p) = (a/q)$.