Do the following exercises from the text:
Section 5.5: 1, 2 (c), (d); 4

1. **(a)** Determine the quadratic residues modulo 11.

▶ **Solution.** Modulo 11 we have $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 5$, $5^2 \equiv 4$. ◀

(b) Determine the quadratic residues modulo 13.

▶ **Solution.** Modulo 13 we have $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 3$, $5^2 \equiv 12$, $6^2 \equiv 10$. ◀

2. If possible, solve the following congruences.

(c) $7x^2 - 4x + 1 \equiv 0 \pmod{11}$

▶ **Solution.** Compute the discriminant $b^2 - 4ac$ modulo 11. In order for the quadratic to be solvable, the equation $y^2 \equiv b^2 - 4ac$ must be solvable. In this case $b^2 - 4ac = 16 - 4 \cdot 7 \cdot 1 = 16 - 28 = -12 \equiv 10 \pmod{11}$. By exercise 1 (a) 10 is not a square modulo 11 so the equation $y^2 \equiv 10$ is not solvable, and hence the original quadratic is not solvable modulo 11. ◀

(d) $7x^2 - 4x + 2 \equiv 0 \pmod{11}$

▶ **Solution.** Modulo 11 $b^2 - 4ac = 16 - 56 = -40 \equiv 4$. Thus, the discriminant equation $y^2 \equiv b^2 - 4ac \pmod{11}$ is $y^2 \equiv 4 \pmod{11}$ which has the two solutions $y = \pm 2 \pmod{11}$. To solve the quadratic, it is necessary to solve $2ax \equiv -b + y \pmod{11}$ or $14x \equiv 4 \pm 2$. Since $4 \cdot 14 = 56 \equiv 1 \pmod{11}$, the two solutions of the quadratic are $x = 4(4+2) \equiv 24 \equiv 2 \pmod{11}$ and $x = 4(4-2) = 8 \equiv 8 \pmod{11}$. ◀

4. If possible solve the following congruences.

(a) $7x^2 - 4x + 2 \equiv 0 \pmod{7}$

▶ **Solution.** Since $7x^2 \equiv 0 \pmod{7}$, the congruence becomes the linear congruence $-4x + 2 \equiv 0 \pmod{7}$, which is equivalent to $4x \equiv 2 \pmod{7}$. Since $4 \cdot 2 \equiv 1 \pmod{7}$, the unique solution is $x \equiv 4 \pmod{7}$. ◀

(b) $7x^2 - 4x + 2 \equiv 0 \pmod{77}$

▶ **Solution.** Since $77 = 7 \cdot 11$, the quadratic congruence is equivalent to the system of two congruences

$$\begin{aligned} 7x^2 - 4x + 2 &\equiv 0 \pmod 7 \\ 7x^2 - 4x + 2 &\equiv 0 \pmod{11} \end{aligned}$$

The first has the solution $x \equiv 4 \pmod 7$ from part (a), while the second has the two solutions $x \equiv 2 \pmod{11}$ and $x \equiv 8 \pmod{11}$ from problem 2(d). Thus, the solutions of the original quadratic are obtained by solving the pair of simultaneous congruences

$$\begin{aligned} x &\equiv 4 \pmod 7 \\ x &\equiv 2,\, 8 \pmod{11}. \end{aligned}$$

Since $2 \cdot 11 - 3 \cdot 7 = 1$, the solutions of these simultaneous congruences modulo 77 are $4 \cdot 2 \cdot 11 + 2(-3)7 = 46$ and $4 \cdot 2 \cdot 11 + 8(-3)7 = -80 \equiv 74 \pmod{77}$. ◀

Section 5.6: 1, 8

1. Determine the quadratic character of the following numbers modulo the prime 379. Note that 307 and 293 are primes.

(a) 3 **(b)** 5 **(c)** 60 **(d)** -1 **(e)** 307 **(f)** 293

▶ **Solution.** (a) $\left(\frac{3}{379}\right) = \left(\frac{379}{3}\right)(-1)^{\frac{1}{2}(3-1)\frac{1}{2}(379-1)} = \left(\frac{379}{3}\right)(-1)^{1\cdot 189} = -\left(\frac{379}{3}\right) = -\left(\frac{3\cdot 126+1}{3}\right) = -\left(\frac{1}{3}\right) = -1$ Thus 3 is a quadratic nonresidue modulo 379.

(b) $\left(\frac{5}{379}\right) = \left(\frac{379}{5}\right)(-1)^{2\cdot 189} = \left(\frac{379}{5}\right) = \left(\frac{4}{3}\right) = 1$ where the next to last equality is because $379 \equiv 4 \pmod 5$ and the last equality is because $4 = 2^2$ is a square. Thus 5 is a quadratic residue modulo 379.

(c) $60 = 2^2 \cdot 3 \cdot 5$ so $\left(\frac{60}{379}\right) = \left(\frac{2^2}{379}\right)\left(\frac{3}{379}\right)\left(\frac{5}{379}\right) = 1 \cdot (-1) \cdot 1 = -1$ from parts (a) and (b). Hence 60 is a quadratic nonresidue modulo 379.

(d)$\left(\frac{-1}{379}\right) = (-1)^{(379-1)/2} = (-1)^{189} = -1$ by Euler's criterion. Hence, -1 is a quadratic nonresidue modulo 379.

(e) $\left(\frac{307}{379}\right) = \left(\frac{379}{307}\right)(-1)^{189\cdot 153} = (-1)\left(\frac{379}{307}\right) = (-1)\left(\frac{72}{307}\right) = (-1)\left(\frac{6^2\cdot 2}{307}\right) = (-1)\left(\frac{6^2}{307}\right)\left(\frac{2}{307}\right) = (-1)(1)(-1) = 1$ where the next to last last equality uses the fact that 6^2 is a square and $307 \equiv 3 \pmod 8$. Thus, 307 is a quadratic residue modulo 379.

(f)$\left(\frac{293}{379}\right) = \left(\frac{379}{293}\right)(-1)^{189\cdot 146} = \left(\frac{379}{293}\right) = \left(\frac{86}{293}\right) = \left(\frac{2}{293}\right)\left(\frac{43}{293}\right) = \left(\frac{2}{293}\right)\left(\frac{293}{43}\right) = \left(\frac{2}{293}\right)\left(\frac{35}{43}\right) = \left(\frac{2}{293}\right)\left(\frac{5}{43}\right)\left(\frac{7}{43}\right) = \left(\frac{2}{293}\right)\left(\frac{43}{5}\right)\left(\frac{43}{7}\right)(-1) = \left(\frac{2}{293}\right)\left(\frac{3}{5}\right)\left(\frac{1}{7}\right)(-1) = (-1)(-1)(1)(-1) = (-1)$ Thus, 293 is a quadratic nonresidue modulo 379. ◀

8. Note that $2717 = 11 \cdot 13 \cdot 19$ and determine if $x^2 \equiv 295 \pmod{2717}$ is solvable.

▶ **Solution.** Since $2717 = 11 \cdot 13 \cdot 19$ and 11, 13, and 19 are pairwise relatively prime, then $x^2 \equiv 295 \pmod{2717}$ is solvable if and only if the system

$$\begin{aligned} x^2 &\equiv 295 \pmod{11} \\ x^2 &\equiv 295 \pmod{13} \\ x^2 &\equiv 295 \pmod{19} \end{aligned}$$

is solvable. Thus, we need to calculate $\left(\frac{295}{11}\right)$, $\left(\frac{295}{13}\right)$, and $\left(\frac{295}{19}\right)$. The first two Legendre symbols are calculated to be 1. But $\left(\frac{295}{19}\right) = \left(\frac{10}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{5}{19}\right) = (-1)\left(\frac{19}{5}\right) = (-1)\left(\frac{4}{5}\right) = -1$. Thus, the last congruence is not solvable and hence the system is not solvable. ◀