Problem Set 3: Quadratic Residues Part 1

14) **(a)** List all of the squares and non-squares in $\mathbb{Z}_{13}$ and $\mathbb{Z}_{19}$.

Solution: Let's make tables again!

$\mathbb{Z}_{13}$

x	±1	±2	±3	±4	±5	±6
x^2 (13)	1	4	9	3	12	10

squares: $1, 3, 4, 9, 10, 12$

non-squares: $2, 5, 6, 7, 8, 11$

$\mathbb{Z}_{19}$

x	±1	±2	±3	±4	±5	±6	±7	±8	±9
x^2 (19)	1	4	9	16	6	17	11	7	5

squares: $1, 4, 5, 6, 7, 9, 11, 16, 17$

non-squares: $2, 3, 8, 10, 11, 12, 13, 14, 18$

(b) For primes $p \in \{7, 11, 13, 17, 19\}$, which ones have -1 as a square in $\mathbb{Z}_p$?

Solution: We have the tables for $7, 11, 13, 19$ from the notes and this solution set. We need the table for $\mathbb{Z}_{17}$.

$\mathbb{Z}_{13}$

x	±1	±2	±3	±4	±5	±6	±7	±8
x^2 (17)	1	4	9	16	8	2	15	13

As $16 \equiv -1 \pmod{17}$ and $-1 \equiv 12 \pmod{13}$, we have that -1 is a square mod p for $p = 13, 17$. ■

(c) Which of the primes $p \in \{7, 11, 13, 17, 19\}$ can be written as $x^2 + y^2$ for non-zero $x, y \in \mathbb{Z}$?

Solution: The squares less than 19 are simply $1, 4, 9, 16$. We have $13 = 9 + 4$ and $17 = 16 + 1$.... and that's it!

(d) Any pattern connecting parts **(b)** and **(c)**?

Solution: The primes which were 1 modulo 4 satisfied the conditions in both parts **(b)** and **(c)**. This isn't a coincidence! ■

15) **(a)** Let p be an odd prime. Solve $x^2 \equiv 1 \pmod{p}$.

Solution: We know that $(-1)^2 \equiv 1^2 \equiv 1 \pmod{p}$. From **Theorem 2** in the Day 3 notes, we conclude that these must be the **only** such solutions. ■

(b) Let $x \in \mathbb{Z}_p^*$ where $x \not\equiv \pm1 \pmod{p}$. Why is $x^{-1} \not\equiv x \pmod{p}$?

Solution: If $x^{-1} \equiv x \pmod{p}$, then as $x \cdot x^{-1} \equiv 1 \pmod{p}$, we have that $x^2 \equiv 1 \pmod{p}$. From part **(a)** we know this is impossible if $x \not\equiv \pm1 \pmod{p}$. □

(c) Using parts **(a)** and **(b)** above, prove the following theorem:

Wilson's Theorem: If $p \in \mathbb{Z}$ is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Hint: This one is still left for an exercise. As a hint, using part **(b)**, you know that you can pair off elements $x \not\equiv \pm 1$ with their inverses. Think about what this means for $(p-1)!$ and how many terms there are in that product.

(d) For $p \equiv 1 \pmod{4}$, set $n = \dfrac{p-1}{2}$. Show that $(n!)^2 \equiv -1 \pmod{p}$ so that you can conclude -1 is a square modulo p.

Proof: First, an essential fact for working modulo 4:

Claim: If $p \equiv 1 \pmod{4}$, then $\dfrac{p-1}{2}$ is even

Proof of claim: If $p \equiv 1 \pmod{4}$, then $p = 4k+1$ for some $k \in \mathbb{Z}$. Then $p-1 = 4k$, so $\dfrac{p-1}{2} = 2k$, and thus is even. ■

With the claim proven, we have that n is even. Recall that $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n-1 \cdot n$. As n is even, we know that

$$(-1) \cdot (-2) \cdot \cdots \cdot (-n) = (-1)^n n! = n!.$$

Modulo p, we have

$$\begin{aligned}(-1) \cdot (-2) \cdot \cdots \cdot (-n) &\equiv (p-1) \cdot (p-2) \cdot \cdots \cdot p-n \\ &\equiv (p-1) \cdot (p-2) \cdot \cdots \cdot \frac{p+1}{2}.\end{aligned}$$

Therefore, we can write $(n!)^2$ modulo p as

$$n! \cdot (-1)^n n! \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \cdots \cdot (p-2) \cdot (p-1)$$

$$\Rightarrow \ (n!)^2 \equiv (p-1)! \equiv -1 \pmod{p} \quad \textit{by Wilson's Theorem}.$$

Therefore, -1 is a quadratic residue modulo any prime that is 1 modulo 4! □

16) **(a)** For each prime $p < 43$, determine whether or not p can be written in the form $x^2 + 3y^2$ for positive integers x and y.

(b) For each prime $p < 43$, determine whether or not -3 is a square modulo p.

Solution: Table for parts **(a)** and **(b)**:

p	2	3	5	7	11	13	17	19	23	29	31	37	41
-3 is a square in $\mathbb{Z}_p$?	Y	N	N	Y	N	Y	N	Y	N	N	Y	Y	N
$p = x^2 + 3y^2$?	N	Y	N	Y	N	Y	N	Y	N	N	Y	Y	N

■

(c) Any pattern connecting parts **(a)** and **(b)**?

Solution: Ignoring $p = 2$ and $p = 3$ (for which there is very good reason), you can observe that the two conditions are aligning perfectly. Let's take a look at where the answer was yes vs no:

- Yes: 7, 13, 19, 31, 37
- No: 5, 11, 17, 23, 29, 41

Since we're working with modular arithmetic, it's reasonable to try to find patterns through that lens! Examining these numbers modulo 3, we note that every prime for which the answer was "Yes" is 1 modulo 3, and every prime for which the answer was "No" is 2 modulo 3! As an exercise, try to formally establish this connection! ■

(d) Can you find a similar connection for primes p which can be written in the form $x^2 + 5y^2$ for positive integers x and y, and whether or not -5 is a square modulo p? Try for primes $p < 110$.

Solution:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
-5 square in $\mathbb{Z}_p$?	Y	Y	Y	Y	N	N	N	N	Y	Y	N	N	Y	Y	Y
$p = x^2 + 5y^2$?	N	N	N	N	N	N	N	N	N	Y	N	N	Y	N	N

p	53	59	61	67	71	73	79	83	89	97	101	103	107	109
-5 square in $\mathbb{Z}_p$?	N	N	Y	Y	N	N	N	Y	Y	N	Y	Y	Y	Y
$p = x^2 + 5y^2$?	N	N	Y	N	N	N	N	N	Y	N	Y	N	N	Y

From the tables, for $p > 7$, we can see that whenever $p = x^2 + 5y^2$ we have that -5 is a residue modulo p, but not conversely. So -5 does not exhibit the same pattern. A pattern for -5 does exist, but requires much more advanced number theory and algebra to establish. ■

17) (a) Prove that $\mathbb{Z}_p^*$ has exactly $\dfrac{p-1}{2}$ quadratic residues.

Proof: Recall from Theorem 2 from the Day 3 notes that if $a \in \mathbb{Z}_p^*$ is a quadratic residue modulo p then $x^2 \equiv a \pmod{p}$ has **EXACTLY** two solutions, and that if b is such a solution, then $\pm b$ are the two unique, distinct solutions.

We've seen before that we can write $\mathbb{Z}_p^* = \left\{\pm 1, \pm 2, ..., \pm\left(\frac{p-1}{2}\right)\right\}$. If $a, b \in \mathbb{Z}_p^*$ are distinct, with $1 \leq a, b \leq \frac{p-1}{2}$, we know from Theorem 2 that $a^2 \not\equiv b^2 \pmod{p}$ (otherwise $a \equiv b$ since $-b > \frac{p-1}{2}$, and $a \equiv b$ contradicts our assumption that they are distinct).

Therefore, $\left\{(\pm 1)^2, (\pm 2)^2, (\pm 3)^2, ..., \left(\pm \frac{p-1}{2}\right)^2\right\}$ is a complete list of (distinct) squares modulo p. As there are $\frac{p-1}{2}$ elements listed, we have that there are exactly $\frac{p-1}{2}$ distinct quadratic residues in $\mathbb{Z}_p^*$. □

(b) Why does $\mathbb{Z}_p^*$ have the same number of quadratic residues as quadratic non-residues?

Solution: We know that $\mathbb{Z}_p^*$ contains $p-1$ elements, and from part **(a)** we know it contains **exactly** $\frac{p-1}{2}$ quadratic residues. Therefore, it contains $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ quadratic non-residues, which is the same value as the number of quadratic residues! ■

Problem Set 4: Quadratic Residues Part 2

18) Use Euler's Criterion to compute $\left(\dfrac{3}{13}\right)$ by hand. Then use Quadratic Reciprocity to compute it. Which route was nicer?

Solution: First, using Euler's Criterion:

$$\begin{aligned}\left(\frac{3}{13}\right) &\equiv 3^{\frac{13-1}{2}} \pmod{13}\\ &\equiv 3^6 \equiv 27^2 \equiv 1^2 \equiv 1 \pmod{13}\,.\end{aligned}$$

Now, using Quadratic Reciprocity:

$$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right)\Big(-1\Big)^{\frac{13-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{1}{3}\right)\cdot 1 = 1.$$

The Euler's Criterion solution given used a nice shortcut about reducing 3^6 using $(3^3)^2$ instead of brute-force calculating 3^6. Even with this shortcut, the Quadratic Reciprocity route is cleaner. ■

19) Prove that $\left(\dfrac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4\,,\\ -1, & p \equiv 3 \pmod 4\,.\end{cases}$

Proof: Let $p \equiv 1 \pmod 4$. Then $p = 4k+1$ for some $k \in \mathbb{Z}$. Using Euler's Criterion, we have

$$\begin{aligned}\left(\frac{-1}{p}\right) &\equiv \Big(-1\Big)^{\frac{p-1}{2}} \pmod p\\ &\equiv \Big(-1\Big)^{\frac{4k+1-1}{2}} \pmod p\\ &\equiv (-1)^{2k} \pmod p\\ &\equiv 1 \pmod p\,,\end{aligned}$$

as $2k$ is an even number. Now, for $p \equiv 3 \pmod 4$, we have $p = 4k+3$ for some $k \in \mathbb{Z}$. Using Euler's Criterion again, we have

$$\begin{aligned}\left(\frac{-1}{p}\right) &\equiv \Big(-1\Big)^{\frac{p-1}{2}} \pmod p\\ &\equiv \Big(-1\Big)^{\frac{4k+3-1}{2}} \pmod p\\ &\equiv \Big(-1\Big)^{\frac{4k+2}{2}} \pmod p\\ &\equiv (-1)^{2k+1} \pmod p\end{aligned}$$

$$\equiv -1 \pmod{p},$$

as $2k+1$ is an odd number. □

20) Suppose that p and q are distinct odd primes. Prove the following equivalent formulation of the law of Quadratic Reciprocity:

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

Proof: The Law of Quadratic Reciprocity states

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)\left(-1\right)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Without loss of generality, suppose that $p \equiv 1 \pmod{4}$ (this is to say, we can interchange the roles of p and q in the following argument and the argument would be identical, so there is no need to repeat ourselves!)

We saw in the proof of **Question 19** that $\left(-1\right)^{\frac{p-1}{2}} = 1$ when $p \equiv 1 \pmod{4}$. Therefore,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)\left(1\right)^{\frac{q-1}{2}} = 1.$$

Now, suppose that $p \equiv q \equiv 3 \pmod{4}$. Again, from the proof of **Question 19**, we saw that if $p \equiv 3 \pmod{4}$, then $\left(-1\right)^{\frac{p-1}{2}} = -1$. This also holds for q since it is also 3 modulo 4. Therefore,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)\left(-1\right)^{q-1}2 = -1.$$ □

21) **(a)** Is 30 a square modulo 101?

(b) Is 105 a square modulo 229?

(c) Is 70 a square modulo 149?

Solution: We will use the properties of the Legendre Symbol and **Theorem 4** for all three questions, along with the nice shortcut in **Question 20**. Note here that all of $101, 149, 229$ are congruent to 1 modulo 4. Therefore, $\left(\frac{p}{149}\right) = \left(\frac{149}{p}\right) \cdot 1$ for any odd prime p (we include the "redundant" $\cdot 1$ here to acknowledge the result of the Law of Quadratic Reciprocity - it is optional to include).

(a) $\left(\frac{30}{101}\right) = \left(\frac{2}{101}\right) \cdot \left(\frac{15}{101}\right)$

$$
\begin{aligned}
&= (-1)\cdot\left(\frac{3}{101}\right)\cdot\left(\frac{5}{101}\right)\\
&= (-1)\cdot\left(\frac{101}{3}\right)\cdot 1\cdot\left(\frac{101}{5}\right)\cdot 1\\
&= (-1)\cdot\left(\frac{2}{3}\right)\cdot\left(\frac{1}{5}\right) = (-1)(-1)(1) = 1.
\end{aligned}
$$

(b)
$$
\begin{aligned}
\left(\frac{105}{229}\right) &= \left(\frac{21}{229}\right)\cdot\left(\frac{5}{229}\right)\\
&= \left(\frac{3}{229}\right)\cdot\left(\frac{7}{229}\right)\cdot\left(\frac{5}{229}\right)\\
&= \left(\frac{229}{3}\right)\cdot 1\cdot\left(\frac{229}{5}\right)\cdot 1\cdot\left(\frac{229}{7}\right)\cdot 1\\
&= \left(\frac{1}{3}\right)\cdot\left(\frac{4}{5}\right)\cdot\left(\frac{5}{7}\right) = 1\cdot 1\cdot -1 = -1.
\end{aligned}
$$

(c)
$$
\begin{aligned}
\left(\frac{70}{149}\right) &= \left(\frac{2}{149}\right)\cdot\left(\frac{5}{149}\right)\cdot\left(\frac{7}{149}\right)\\
&= (-1)\cdot\left(\frac{149}{5}\right)\cdot 1\cdot\left(\frac{149}{7}\right)\cdot 1\\
&= (-1)\cdot\left(\frac{4}{5}\right)\cdot\left(\frac{2}{7}\right) = (-1)\cdot(1)\cdot(1) = -1.
\end{aligned}
$$

Therefore, 30 is a square modulo 101, but 105 is not a square modulo 229 and 70 is not a square modulo 149. ■

22) Prove that the Legendre symbol is multiplicative using Euler's Criterion.

Hint: Use the multiplication property of exponents; that is, $(ab)^x = a^x b^x$. ■

23) Let p be an odd prime. Prove that if $a, b \in \mathbb{Z}_p^*$ are non-squares modulo p, then ab is a square modulo p.

Hint: Use the multiplicative property of the Legendre symbol! ■

24) **(a)** Let $p \geq 11$ be prime. Prove that $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)$.

Proof: Using the multiplicative property of the Legendre symbol, we have

$$\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)\cdot\left(\frac{4}{p}\right) = \left(\frac{2}{p}\right)\cdot\left(\frac{2^2}{p}\right) = \left(\frac{2}{p}\right)\cdot 1 = \left(\frac{2}{p}\right). \qquad \square$$

Note: The above proof actually works for any odd prime p; we chose $p \geq 11$ so that $8 \in \mathbb{Z}_p$.

(b) Let p be a prime, let $a \in \mathbb{Z}_p^*$ and let k be an odd positive integer. Prove that $\left(\frac{a^k}{p}\right) = \left(\frac{a}{p}\right)$.

Proof: If k is odd, then $k = 2m + 1$ for some $m \in \mathbb{Z}$. Using similar logic to what was used in part **(a)**, we have

$$\left(\frac{a^k}{p}\right) = \left(\frac{a^{2m+1}}{p}\right) = \left(\frac{a^{2m}}{p}\right) \cdot \left(\frac{a}{p}\right) = 1 \cdot \left(\frac{a}{p}\right) = \left(\frac{a}{p}\right). \ \square$$

Note: We can also simplify these proofs further! As the Legendre symbol is multiplicative, you can prove the following:

$$\left(\frac{a^k}{p}\right) = \left(\frac{a}{p}\right)^k.$$

25) Prove Euler's Criterion.
Hint: Start with the statement of Fermat's Little Theorem and use a difference of squares!

Much like Wilson's Theorem, we won't spoil this here! It is left as an exercise. The hint above should help!