Problem Set 3: Quadratic Residues Part 1

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

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

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

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

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

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

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

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

(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.

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.

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

(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 $p < 110$.

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

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

Problem Set 4: Quadratic Residues Part 2

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

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

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

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

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

(b) Is 105 a square modulo 229?

(c) Is 70 a square modulo 149?

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

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.

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

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

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