Homework 13: Due Monday, April 25

Problem 1:
a. Using repeated squaring, reducing as you go, compute the element of $\{1, 2, \dots, 40\}$ that each of 5^1, 5^2, 5^4, 5^8, and 5^{16} is congruent to modulo 41.
b. Using your computations from part (a), determine whether $5^{20} \equiv 1 \pmod{41}$ or $5^{20} \equiv -1 \pmod{41}$.
c. Is 5 a quadratic residue modulo 41? Explain.

Problem 2: Show that $19 \nmid 4n^2 + 4$ for all $n \in \mathbb{Z}$.

Problem 3:
a. Let $p \in \mathbb{N}^+$ be a prime with $p \notin \{2, 3\}$. Explain why either $p \equiv 1 \pmod{6}$ or $p \equiv 5 \pmod{6}$.
b. Show that there are infinitely primes $p \in \mathbb{N}^+$ with $p \equiv 5 \pmod{6}$.

Problem 4: Show that if p is an odd prime, then

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Problem 5: Let p be an odd prime, and let $a, b \in \mathbb{Z}$ with $ab \equiv 1 \pmod{p}$.
a. If a is a quadratic residue modulo p, show that b is also a quadratic residue modulo p.
b. If a is a quadratic nonresidue modulo p, is b also a quadratic nonresidue modulo p? Explain.
c. If a is a quadratic residue modulo p, is $-a$ also a quadratic residue modulo p? Explain.

Problem 6: Let p be a prime with $p \geq 11$.
a. Show that at least one of 2, 5, or 10 is a quadratic residue modulo p.
b. Show that there are always two consecutive numbers in $\{1, 2, \dots, p-1\}$ that are quadratic residues modulo p.