Math 445 — Problem Set #4
Due: Friday, September 29 by 7 pm, on Canvas

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. If you do work with others, I ask that you write something along the top like "I collaborated with Steven Smale on problems 1 and 3". If you use a reference, indicate so clearly in your solutions. In short, be intellectually honest at all times. Please write neatly, using complete sentences and correct punctuation. Label the problems clearly.

(1) Use quadratic reciprocity and its variants to determine if each of the following is a square modulo 257 (which is prime):
- -2
- 59
- 53

(2) The number $p = 892,371,481 = 1 + 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ is prime. (You do not need to check this.) Show that $\left(\frac{n}{p}\right) = 1$ for $0 < n < 29$. Deduce that there is no primitive root $[n]$ in $\mathbb{Z}_p$ with $0 < n < 29$.

(3) Show that if p is an odd prime, then 5 is a square modulo p if and only if $p \equiv \pm 1 \pmod 5$.

(4) Use Gauss' Lemma to prove that if $p \equiv 7 \pmod 8$, then 2 is a quadratic residue modulo p. (This is the $p \equiv -1 \pmod 8$ case of QR part 2.)

(5) Explicit square roots modulo some primes:
  (a) Show that[1] if $p \equiv 3 \pmod 4$ and a is a quadratic residue modulo p, then $a^{(p+1)/4}$ is a square root of a modulo p.
  (b) Show that if $p \equiv 5 \pmod 8$ and a is a quadratic residue modulo p, then either $a^{(p+3)/8}$ or $(2a)(4a)^{(p-5)/8}$ is a square root of a modulo p.
  (c) Use parts (a) and (b) to find square roots of $[13]_{23}$ and $[6]_{29}$.

The remaining problem is only required for Math 845 students, though all are encouraged to think about them.

(6) The nth **Fermat number** is given by $F_n = 2^{2^n} + 1$. The first four Fermat numbers are prime; Fermat thought $F_5 = 2^{2^5} + 1 = 4294967297$ was too, but about a hundred years later, Euler factored it as a product of two primes $641 \cdot 6700417$. In this problem, we will prove **Pépin's test**: For $n > 0$, F_n is prime if and only if $3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}$.
  (a) Show[2] that if F_n is prime, then $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.
  (b) Show[3] that if $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$ then F_n is prime.
  (c) Use Pépin's test to verify that F_3 is prime.

---

[1] Hint: Use Euler's criterion

[2] Hint: Apply Euler's criterion and QR.

[3] Hint: Let p be a prime factor of F_n, which necessarily is odd. Show that the order of $[3]$ in $\mathbb{Z}_p^\times$ is exactly $F_n - 1$.