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

We compute

$$\begin{aligned}\left(\frac{-2}{257}\right) &= \left(\frac{-1}{257}\right)\left(\frac{2}{257}\right)\\ &= 1\cdot 1 && \text{since } 257\equiv 1 \pmod 4 \text{ and } 257 \equiv 1 \pmod 8,\\ &= 1\end{aligned}$$

so -2 is a square modulo 257.

We compute

$$\begin{aligned}\left(\frac{59}{257}\right) &= \left(\frac{257}{59}\right) && \text{since } 257\equiv 1 \pmod 4\\ &= \left(\frac{21}{59}\right) = \left(\frac{3}{59}\right)\left(\frac{7}{59}\right)\\ &= -\left(\frac{59}{3}\right)\cdot -\left(\frac{59}{7}\right) && \text{since } 59, 3, 7 \equiv 3 \pmod 4,\\ &= \left(\frac{59}{3}\right)\cdot\left(\frac{59}{7}\right) = \left(\frac{2}{3}\right)\cdot\left(\frac{3}{7}\right) = -1\cdot -1 = 1\end{aligned}$$

so 59 is a square modulo 257.

We compute

$$\begin{aligned}\left(\frac{53}{257}\right) &= \left(\frac{257}{53}\right) && \text{since } 257\equiv 1 \pmod 4\\ &= \left(\frac{45}{53}\right) = \left(\frac{3^2}{53}\right)\cdot\left(\frac{5}{53}\right) = 1\cdot\left(\frac{53}{5}\right) && \text{since } 53\equiv 1 \pmod 4\\ &= \left(\frac{3}{5}\right) = -1\end{aligned}$$

so 53 is not a square modulo 257.

(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 $0 < n < 29$.

We will show that $2, 3, 5, 7, 11, 13, 17, 19, 23$ are all squares modulo p. For $p = 2$, we apply Quadratic Reciprocity "part 2": since $p \equiv 1 \pmod 8$, we have $\left(\frac{2}{p}\right) = 1$, so 2 is indeed a square. For each odd prime q listed above, note that $p \equiv 1 \pmod 4$ and that $p \equiv 1 \pmod q$. Thus, $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1$, so each such q is a square modulo p. Then, any integer $0 < n < 29$ has a prime factorization involving only the primes 2 and q on the list above; thus $\left(\frac{n}{p}\right)$ can be written as a product, all of whose factors are 1. We deduce that each such n is a square modulo p.

Now, any square cannot be a primitive root: by Euler's criterion, its order is at most $(p-1)/2 < \varphi(p)$. We conclude that no such n can be a primitive root.

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

By quadratic reciprocity, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. The only squares modulo 5 are ± 1, so the result follows.

(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.)

We apply Gauss' Lemma, with $a = 2$ in the notation of the worksheet. Write $p = 8k+7$ for some k, so, in the notation of the Lemma, $p' = 4k+3$. We take the sequence of integers

$$2, 4, \ldots, 2(4k+3).$$

The elements

$$2, 4, \ldots, 4k+2$$

are all in the range $[-p', p']$. For each of the elements

$$4k+4, \ldots, 8k+6$$

subtracting p yields elements

$$-(4k+3), \ldots, -1$$

that are all in the range $[-p', p']$. Thus, the number of negative elements is the number of elements in the latter list, which is $2k+2$. Since this is even, Gauss' Lemma guarantees that $a = 2$ is a square.

(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 $[6]_{29}$.

(a) Write $p = 4k+3$. By Euler's criterion, since a is a square, $1 \equiv a^{(p-1)/2} = a^{2k+1} \pmod p$. Then

$$(a^{(p+1)/4})^2 = (a^{k+1})^2 = a^{2k+2} = a^{2k+1}a \equiv a \pmod p,$$

showing that $a^{(p+1)/4}$ is a square root of a modulo p.

[1] Hint: Use Euler's criterion

(b) Write $p = 8k+5$. By Euler's criterion, since a is a square, $1 \equiv a^{(p-1)/2} = a^{4k+2} \pmod{p}$. Since $(a^{2k+1})^2 = a^{4k+2}$, we must have $a^{2k+1} \equiv \pm 1 \pmod{p}$.
Suppose first that $a^{2k+1} \equiv 1 \pmod{p}$. Then

$$(a^{(p+3)/8})^2 \equiv (a^{k+1})^2 \equiv a^{2k+2} \equiv a^{2k+1}a \equiv a \pmod{p},$$

so $a^{(p+3)/8}$ is a square root of a modulo p. On the other hand, if $2^{(p-1)/2} \equiv -1 \pmod{p}$ by Euler's criterion and QR part 2. Then $a^{2k+1} \equiv -1 \pmod{p}$, then

$$\begin{aligned}((2a)(4a)^{(p-5)/8})^2 &\equiv ((2a)(4a)^k)^2 \equiv 2^{4k+2}a^{2k+2} \\ &\equiv 2^{(p-1)/2} \cdot -1 \cdot a \equiv -1 \cdot -1 \cdot a \equiv a \pmod{p},\end{aligned}$$

so $a^{(p+3)/8}$ is a square root of a modulo p.

(c) Since $23 \equiv 3 \pmod{4}$, we use (a) to compute $[13]^6 = [6]$ is a square root of $[13]$ in $\mathbb{Z}_{23}$. Since $29 \equiv 5 \pmod{8}$, we use (b) to give two candidates: [20] and [8]. We check that $[20]^2 \neq [6]$ and $[8]^2 = [6]$ in $\mathbb{Z}_{29}$, so [8] is a square root of [6].

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.

(a) Suppose that F_n is prime. Then Euler's criterion says that $3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \pmod{F_n}$. But, since $F_n \equiv 1 \pmod{4}$, by quadratic reciprocity, $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$. We have $2^{2^n} \equiv 1 \pmod{3}$, so $F_n \equiv 2 \pmod{3}$, and hence $\left(\frac{F_n}{3}\right) = -1$. We conclude that $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$ in this case.

(b) Suppose that $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$. Let p be a prime factor of F_n, which necessarily is odd. Then $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{p}$. Squaring both sides, $3^{F_n - 1} \equiv 1 \pmod{p}$, so the order of [3] in $\mathbb{Z}_p^\times$ divides $F_n - 1 = 2^{2^n}$. Thus, the order of [3] in $\mathbb{Z}_p^\times$ is a power of 2. But, $3^{\frac{F_n-1}{2}} \equiv -1$ implies that the order of [3] is not $2^{2^n - 1}$. Since any proper divisor of 2^{2^n} divides $2^{2^n - 1}$, we deduce that the order of [3] is exactly $2^{2^n} = F_n - 1$. But the order of [3] is at most $p - 1$, so $p - 1 \geq F_n - 1$, forcing $p = F_n$, and hence that F_n is prime.

(c) We have $F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$. Then $[3]^{(F_3 - 1)/2} = [3]^{128}$. We compute $3^{128} \equiv -1 \pmod{257}$, so 257 is prime by Pépin's test.

---

[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 $F_n - 1$.