**Math 445 — Problem Set #3**
**Due: Tuesday, September 19 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) Using methods from this class, find all integers $x$ that satisfy the congruences:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{8}. \end{cases}$$

(2) Compute[1] the last three base ten digits of $11^{17^{1923}}$.

(3) Computing (some) roots in $\mathbb{Z}_n$:
   (a) Suppose we are given a congruence equation of the form $a^m \equiv b \pmod{n}$, with $a$ and $n$ coprime. Given integers $c, d$ such that $cm + d\varphi(n) = 1$, show that $b^c \equiv a \pmod{n}$.
   (b) Use this to find a cube root of $[7]$ in $\mathbb{Z}_{101}$, and a seventh root of $[3]$ in $\mathbb{Z}_{200}$.
   (c) Explain why this method will never help us find square roots in $\mathbb{Z}_p$ for $p$ an odd prime.

(4) Let $G$ be a finite group and $g \in G$. Suppose that $g^n = 1$ for some positive integer $n$, where $1 \in G$ is this identity element. Show that the order of $g$ divides $n$.

(5) Prove that if $p$ and $q$ are distinct odd primes, there is no primitive root in $\mathbb{Z}_{pq}$.

---

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

(6) Fermat and Euler without the fine print:
   (a) Fermat's little theorem is often stated as: Let $p$ be a prime, and $a$ any integer. Then $a^p \equiv a \pmod{p}$. Deduce this, perhaps with the help of our version.
   (b) Show that if $n$ is a product of distinct primes, then for any integer $a$, $a^{\varphi(n)+1} \equiv a \pmod{n}$.
   (c) Find a counterexample to the statement: if $n > 1$ is an integer, then for any integer $a$, $a^{\varphi(n)+1} \equiv a \pmod{n}$.

(7) Prove[2] that if $p$ is an odd prime and $n > 0$, then there is a primitive root in $\mathbb{Z}_{p^n}$.

---

[1] Note that the standard convention for double exponents is that $a^{b^c}$ means $a^{(b^c)}$ and not $(a^b)^c = a^{bc}$. Also, Nebraska beat Iowa State 26–14 on Nov 17, 1923.

[2] One possibility is to follow these steps (but please write your proof in a self-contained form):
(a) We already know this is true when $n = 1$. For $n = 2$, first show that if $[r]_p$ is a primitive root in $\mathbb{Z}_p$, then the order of $[r]_{p^2}$ in $\mathbb{Z}_{p^2}^\times$ is either $p - 1$ or $p(p - 1)$.
(b) Show that if $[r]_p$ is a primitive root in $\mathbb{Z}_p$, then either $[r]_{p^2}$ or $[r + p]_{p^2}$ is a primitive root in $\mathbb{Z}_{p^2}$.
(c) Show that if $r \in \mathbb{Z}$ is such that $[r]_p$ is a primitive root in $\mathbb{Z}_p$ and $[r]_{p^2}$ is a primitive root in $\mathbb{Z}_{p^2}$, then $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ for any $k \geq 2$.
(d) Conclude the proof.