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:

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

First we need to compute an inverse of $8 \cdot 5 \equiv 1$ modulo 3 (1 works), an inverse of $8 \cdot 3 \equiv 4$ modulo 5 (4 works), and an inverse of $5 \cdot 3 \equiv 7$ modulo 8 (7 works. Then a particular solution is $1 \cdot 1 \cdot 40 + 2 \cdot 4 \cdot 24 + 3 \cdot 7 \cdot 15 = 547$ and the general solution is $547 + 3 \cdot 5 \cdot 8k = 547 + 120k$.

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

By Euler's Theorem, $11^{\varphi(1000)} \equiv 1 \pmod{1000}$. Using the factorization $1000 = 2^3 \cdot 5^3$, we compute $\varphi(1000) = (2-1) \cdot 2^2 \cdot (5-1) \cdot 5^2 = 400$. Thus, if $17^{1923} \equiv a \pmod{400}$, then $11^{17^{1923}} \equiv 11^a \pmod{1000}$.

Now, by Euler's Theorem, $17^{\varphi(400)} \equiv 1 \pmod{400}$. Using the factorization $400 = 2^4 \cdot 5^2$, we compute $\varphi(400) = (2-1) \cdot 2^3 \cdot (5-1) \cdot 5 = 160$. Thus, if $1923 \equiv b \pmod{160}$, then $17^{1923} \equiv 17^b \pmod{400}$.

We have $1923 \equiv 3 \pmod{160}$, so $17^{1923} \equiv 17^3 \equiv 113 \pmod{400}$. So, $11^{17^{1923}} \equiv 11^{113} \pmod{1000}$. This is now something some online calculators can deal with, or more concretely, we can repeatedly square:

$$\begin{aligned} 11^2 &\equiv 121 \\ 11^4 &\equiv 121^2 \equiv 641 \\ 11^8 &\equiv 641^2 \equiv 881 \\ 11^{16} &\equiv 881^2 \equiv 161 \\ 11^{32} &\equiv 161^2 \equiv 921 \\ 11^{64} &\equiv 921^2 \equiv 241 \end{aligned}$$

and then

$$11^{113} = 11^{64} \cdot 11^{32} \cdot 11^{16} \cdot 11^1 \equiv 931 \pmod{1000}.$$

So, the last digits are 931.

(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 $\mathbb{Z}_{200}$.

[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.

(c) Explain why this method will never help us find square roots in $\mathbb{Z}_p$ for p an odd prime.

(a)
$$b^c \equiv a^{mc} \equiv a^{1-d\varphi(n)} \equiv a(a^{\varphi(n)})^d \equiv a \pmod{n},$$
using Euler's Theorem.

(b) We use the Euclidean algorithm to write $-33 \cdot 3 + 1 \cdot 100 = 1$, so by the first part (and Fermat/Euler) $[7]^{-33} \equiv [7]^{67} \equiv [8]$ is a cube root of $[7]$. Similarly for the other, we find $-2 \cdot 80 + 23 \cdot 7 = 1$, so $[3]^2 3 \equiv [27]$ is a seventh root of $[3]$.

(c) We have $\varphi(p) = p - 1$ is even, so 2 is not coprime with $\varphi(p)$.

(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.

Suppose that $g^n = 1$ and that d is the order of g. Write $n = de + r$ with $0 \leq r < d$. Then singe $g^d = 1$, we have $1 = g^n = g^{de+r} = (g^d)^e g^r = 1^e g^r = g^r$. By definition of order, since $r < d$, we must have that $r = 0$, so $d|n$.

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

Write $\varphi(p) = p - 1 = 2a$ and $\varphi = q - 1 = 2b$. We claim that every element of $\mathbb{Z}_{pq}^\times$ has order at most $2ab < (2a)(2b) = \varphi(pq)$; from this claim, the statement follows since a primitive root would have order $\varphi(pq)$ by definition.

Take $x = [r] \in \mathbb{Z}_{pq}^\times$. By Fermat's Little Theorem, we have $r^{p-1} \equiv 1 \pmod{p}$, and $r^{q-1} \equiv 1 \pmod{q}$. Then, $r^{2ab} \equiv (r^{p-1})^b \equiv 1 \pmod{p}$ and $r^{2ab} \equiv (r^{q-1})^a \equiv 1 \pmod{q}$. Since p, q are coprime, by the uniqueness part of the Chinese Remainder Theorem, we must have $r^{2ab} \equiv 1 \pmod{pq}$, and hence the order of $x = [r]$ is at mote $2ab$, as claimed.

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, $a^{\varphi(n)+1} \equiv a \pmod{n}$.

(a) We proceed by cases. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ by FLT, so $a^p \equiv a \pmod{p}$. If $p \mid a$, then $a \equiv 0 \pmod{p}$, and hence $a^p \equiv 0 \equiv a \pmod{p}$.

(b) Write $n = p_1 p_2 \cdots p_k$. Let $N = \varphi(n) + 1$.
We claim that $a^N \equiv a \pmod{p_i}$ for each i. To show this, fix i. Note that $N \equiv 1 \pmod{p_i - 1}$, so write $N = d_i(p_i - 1) + 1$. If $p_i \nmid a$, we have $a^{p_i - 1} \equiv 1 \pmod{p}$ by FLT, so $a^N \equiv a^{d_i(p_i-1)+1} \equiv (a^{p_i-1})^{d_i} a \equiv a \pmod{p_i}$. If $p_i \mid a$, we have $a^N \equiv 0 \equiv a \pmod{p_i}$. This shows the claim.
Now, since $a^N \equiv a \pmod{p_i}$ for each i, by the uniqueness part of CRT, we have $a^N \equiv a \pmod{n}$.

(c) Take $n = 4$ and $a = 2$; then $\varphi(n) = 2$ and $a^{\varphi n+1} = a^3 \equiv 0 \not\equiv a$.

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

Note that the case $n = 1$ is a Theorem from class.

We address the case $n = 2$ next. Let $r \in \mathbb{Z}$ be a unit modulo p and suppose that r is a primitive root modulo p, which, as we just said, exists. Since $\varphi(p^2) = p(p-1)$, the order of r modulo p^2 divides $p(p-1)$. Since $r^p \equiv r \not\equiv 1 \pmod{p}$, we have $r^p \not\equiv 1 \pmod{p^2}$, so the order is not 1 or p. Thus, the order of r modulo p^2 is either $p-1$ or $p(p-1)$. That is, a primitive root modulo p is either also a primitive root modulo p^2 or has order $p-1$ modulo p^2.

Suppose that r is a primitive root modulo p and its order modulo p^2 is $p-1$. Then

$$(r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + \boxed{\text{multiples of } p^2} \equiv 1 - r^{p-2}p \pmod{p^2}.$$

But $1 - r^{p-2}p$ cannot be a multiple of p^2, since this would imply $p|(1 - r^{p-2}p)$ and $p|1$, which is a contradiction. But $r+p$ is a primitive root modulo p, and its order is not $p-1$, so it must be a primitive root modulo p^2. This concludes the case $n = 2$.

Now we claim that if r is a primitive root modulo p and p^2, then

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$$

for any $k \geq 2$. We proceed by induction on k, with base case $k = 2$ a consequence of the definition of primitive root modulo p^2. Write $r^{p^{k-2}(p-1)} = a + bp^k$ with $0 \leq a < p^k$. Then

$$\begin{aligned} r^{p^{k-1}(p-1)} &= (r^{p^{k-2}(p-1)})^p = (a + p^k b)^p \\ &= a^p + pa^{p-1}p^k b + \boxed{\text{multiples of } p^{2k}} \equiv a^p \pmod{p^{k+1}}. \end{aligned}$$

By the Lemma we prove below, $a^p \not\equiv 1 \pmod{p^{k+1}}$, which completes the induction, and the proof of the claim.

Finally, let r be a primitive root modulo p and p^2. We note that the order of r in $\mathbb{Z}_{p^n}^\times$ divides $\varphi(p^n) = p^{n-1}(p-1)$. For any k, we can write $p^k = e_k(p-1)+1$, so $r^{p^k} \equiv r^{e_k(p-1)+1} \equiv r \not\equiv 1 \pmod{p}$, so $r^{p^k} \not\equiv r^{p^k} \pmod{p^n}$, and thus the order of r is $(p-1)p^k$ for some k. But by previous claim, the order is not $(p-1)p^k$ for $k < n-1$, so r must be a primitive root modulo p^n. □

Lemma: Let a be an integer not divisible by some prime p. If $a \not\equiv 1 \pmod{p^k}$, then $a^p \not\equiv 1 \pmod{p^{k+1}}$.

Proof: We proceed by induction on k. For the base case $k = 1$, by FLT, $a^p \equiv a \pmod{p}$, so $a^p \equiv 1 \pmod{p^2}$ implies $a^p \equiv 1 \pmod{p}$ implies $a \equiv 1 \pmod{p}$.

For the inductive step, suppose for the sake of contradiction that $a \not\equiv 1 \pmod{p^k}$ and $a^p \equiv 1 \pmod{p^{k+1}}$. By the IH, since $a^p \equiv 1 \pmod{p^k}$, we have $a \equiv 1 \pmod{p^{k-1}}$, and we can write $a = 1 + p^{k-1}t$ for some t. Then

$$a^p = (1 + p^{k-1}t)^p = 1 + pp^{k-1}t + \boxed{\text{multiples of } p^{2k-2}} \equiv 1 \pmod{p^k},$$

a contradiction. □

[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.