Math 322 Fall 2017
Number Theory HW 10 Solutions
Due **Wednesday** November 29

There is no starred problem this week!

For the remainder of these problems, I encourage you to collaborate with your classmates, as well as to discuss them with me.

1. Let $k \geq 3$ be an integer. Then prove that

$$\text{ord}_{2^k} 5 = \phi(2^k)/2 = 2^{k-2}.$$

(Hint: we know that the order divides 2^{k-1} and is not equal to 2^{k-1}; the largest it can possibly be is 2^{k-2}. So we just have to prove it's no smaller).

Solution:

Proof. We know that $5^{2^{k-2}} \equiv 1 \mod 2^k$ by a lemma from class. So we know $\text{ord}_{2^k} 5 | \phi(2^k)/2$; we need to show this is an equality. So we just need to show that $\text{ord}_{2^k} 5 \not| 2^{k-3}$.

We claim that for $k \geq 3$, that

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \not\equiv 1 \mod 2^k.$$

We prove this by, what else, induction.

For $k = 3$ we see that $5^{2^{k-3}} = 5^1 = 5 \equiv 1 + 4 \mod 2^3$.

Now assume that

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \mod 2^k.$$

Then there is an integer d such that $5^{2^{k-3}} = 1 + 2^{k-1} + d2^k$. Squaring both sides gives

$$\begin{aligned} 5^{2^{k-2}} &= (1 + 2^{k-1})^2 + 2(1 + 2^{k-1})d2^k + (d2^k)^2 \\ &\equiv (1 + 2^{k-1})^2 \mod 2^{k+1} \\ &\equiv 1 + 2 \cdot 2^{k-1} + 2^{2k-2} \mod 2^{k+1} \\ &\equiv 1 + 2^k \mod 2^{k+1} \end{aligned}$$

as desired. □

2. Let m be a natural number with primitive root r, and let a, b be relatively prime to m. Then prove that:

   (a) $\operatorname{ind}_r 1 \equiv 0 \mod \phi(m)$

   (b) $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \mod \phi(m)$

   (c) $\operatorname{ind}_r a^k \equiv k \operatorname{ind}_r a \mod \phi(m)$.

   Solution:

   (a) Since r is a primitive root modulo m, we know that $\phi(m)$ is the smallest positive integer such that $r^x \equiv 1 \mod m$, so $\operatorname{ind}_r 1 = \phi(m) \equiv 0 \mod \phi(m)$.

   (b) We observe that

$$\begin{aligned} r^{\operatorname{ind}_r(ab)} &\equiv ab \mod m \\ r^{\operatorname{ind}_r a + \operatorname{ind}_r b} &\equiv r^{\operatorname{ind}_r a} r^{\operatorname{ind}_r b} \equiv ab \mod m \\ \text{thus } r^{\operatorname{ind}_r(ab)} &\equiv r^{\operatorname{ind}_r a + \operatorname{ind}_r b} \mod m \end{aligned}$$

   and we know that if the powers are congruent modulo m then the exponents are congruent modulo $\phi(m)$. Thus $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \mod \phi(m)$.

   (c) The proof is similar to before:

$$\begin{aligned} r^{\operatorname{ind}_r a^k} &\equiv a^k \mod m \\ r^{k \operatorname{ind}_r a} &\equiv (r^{\operatorname{ind}_r a})^k \equiv a^k \mod m \end{aligned}$$

   and thus the powers are equivalent mod m, and hence the exponents are equivalent mod $\phi(m)$.

3. Find all solutions to $7x^9 \equiv 4 \mod 17$.

   Solution:

$$\begin{aligned} \operatorname{ind}_3(7x^9) &\equiv \operatorname{ind}_3 4 \mod 16 \\ \operatorname{ind}_3 7 + 9 \operatorname{ind}_3 x &\equiv \operatorname{ind}_3 4 \mod 16 \\ 11 + 9 \operatorname{ind}_3 x &\equiv 12 \mod 16 \\ \operatorname{ind}_3 x &\equiv 1/9 \equiv 9 \mod 16 \\ x &\equiv 14 \mod 17. \end{aligned}$$

4. Find all solutions to $5^x \equiv 4 \mod 17$.

   Solution:

$$\begin{aligned} \operatorname{ind}_3(5^x) &\equiv \operatorname{ind}_3 4 \mod 16 \\ x \cdot 5 &\equiv 12 \mod 16 \\ x &\equiv 12 \cdot (-3) \equiv 12 \mod 16. \end{aligned}$$

5. (a) Compute the index base 2 of 15 modulo 19. **Solution:** $2^{11} \equiv 15 \mod 19$ so $\operatorname{ind}_2 15 = 11$.

   (b) Compute the index base 3 of 15 modulo 19.
   Solution: $3^5 \equiv 15 \mod 19$ so $\operatorname{ind}_3 15 \equiv 5 \mod 19$.

   (c) Find all natural numbers less than 13 which are squares modulo 13.
   Solution: 1, 4, 9, 3, 12, 10

   (d) Find all natural numbers less than 13 which are cubes modulo 13.
   Solution: 1, 8, 12, 5