MATH 406 (JWG) Exam 2 Spring 2021 Sample 2

---

1. Calculate:

   (a) $\phi(2^3 \cdot 5 \cdot 11^2)$
   Solution:
   Just use the rules!

   (b) $\sigma(200)$
   Solution:
   Find the prime factorization and then just use the rules!

   (c) $\tau(2000)$
   Solution:
   Find the prime factorization and then just use the rules!

2. Use Wilson's Theorem to find the remainder when 16! is divided by 19.

   Solution:

   We have:

$$\begin{aligned}
18! &\equiv -1 \mod 19 \\
(18)(17)16! &\equiv -1 \mod 19 \\
(-1)(-2)16! &\equiv -1 \mod 19 \\
(-2)16! &\equiv 1 \mod 19 \\
(-10)(-2)16! &\equiv -10 \mod 19 \\
(20)16! &\equiv 9 \mod 19 \\
16! &\equiv 9 \mod 19
\end{aligned}$$

3. Find all n with $\phi(n) = 16$.

   Solution:

   We've done a bunch of these by now!

4. Show that 25 is a Fermat Pseudoprime to the base 7.

   Solution:

   Just show that $7^{24} \equiv 1 \mod 25$.

5. An abundant number is a number n with $\sigma(n) > 2n$. Prove that there are infinitely many even abundant numbers by finding one abundant number and by showing that if n is abundant and a prime p satisfies $p \nmid n$ then pn is also abundant.

   Solution:

   For example 12 is abundant since $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28 > 2(12)$.

   If $p \nmid n$ then $\gcd(p, n) = 1$ and so

$$\sigma(pn) = \sigma(p)\sigma(n) = (p+1)\sigma(n) > (p+1)2n = 2np + 2n > 2pn$$

   thus pn is abundant.

6. A partial table of indices for 2, a primitive root of 13, is given here:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2 a$	12	1	4	2	9	5	11	3	a	b	7	6

(a) Find a and b with justification.
Solution:
First:

$$a = \text{ind}_2 9 = \text{ind}_2 3^2 = 2\text{ind}_2 3 = 2(4) = 8$$

Second:

$$b = \text{ind}_2(10) = \text{ind}_2(2 \cdot 5) = \text{ind}_2 2 + \text{ind}_2 5 = 1 + 9 = 10$$

(b) Use the table to solve the congruence $3^{2x+1} \equiv 9 \mod 13$.
Solution:
We have:

$$\begin{aligned}
3^{2x+1} &\equiv 9 \quad \text{mod } 13 \\
\text{ind}_2 3^{2x+1} &\equiv \text{ind}_2 9 \quad \text{mod } \phi(13) = 12 \\
(2x+1)\text{ind}_2 3 &\equiv \text{ind}_2 9 \quad \text{mod } 12 \\
(2x+1)(4) &\equiv 8 \quad \text{mod } 12 \\
8x + 4 &\equiv 8 \quad \text{mod } 12 \\
8x &= 4 \quad \text{mod } 12 \\
2x &= 1 \quad \text{mod } 3 \\
x &= 1 \quad \text{mod } 3 \\
x &= 1, 4, 7, 11 \quad \text{mod } 12
\end{aligned}$$

Note: I didn't ask for the solution mod 12 so you could have left it mod 3.

(c) Use the table to solve the congruence $7x^5 \equiv 3 \mod 13$.
Solution:
We have:

$$\begin{aligned}
7x^5 &\equiv 3 \quad \text{mod } 13 \\
\text{ind}_2 7x^5 &\equiv \text{ind}_2 3 \quad \text{mod } \phi(13) = 12 \\
\text{ind}_2 7 + 5\text{ind}_2 x &\equiv 4 \quad \text{mod } 12 \\
11 + 5\text{ind}_2 x &\equiv 4 \quad \text{mod } 12 \\
5\text{ind}_2 x &\equiv 5 \quad \text{mod } 12 \\
\text{ind}_2 x &\equiv 1 \quad \text{mod } 12 \\
x &\equiv 2 \quad \text{mod } 13
\end{aligned}$$

7. Prove that if $\text{ord}_n a = hk$ then $\text{ord}_n \left(a^h\right) = k$.
Note: The intention is to do this without the theorem from class.
Solution:
First note that $\left(a^h\right)^k \equiv a^{hk} \equiv 1 \mod n$. Then suppose that $\left(a^h\right)^j \equiv 1 \mod n$ so then $a^{hj} \equiv 1$ mod n so that $hj \geq hk$ so that $j \geq k$. Thus $\text{ord}_n \left(a^h\right) = k$.

8. Let r be a primitive root for an odd prime p. Prove that $\text{ind}_r(p-1) = \frac{1}{2}(p-1)$.

   Solution:

   We know by Euler's Theorem that:

   $$r^{p-1} \equiv 1 \mod p$$

   Thus:

   $$p \mid r^{p-1} - 1 = \left(r^{\frac{1}{2}(p-1)} + 1\right)\Big)r^{\frac{1}{2}(p-1)} - 1\Big)$$

   So p divides one of them. If $p \mid r^{\frac{1}{2}(p-1)} - 1$ then $r^{\frac{1}{2}(p-1)} \equiv 1 \mod p$ which contradicts the fact that r is a primitive root. Thus we know that $p \mid r^{\frac{1}{2}(p-1)} - 1$ and so $r^{\frac{1}{2}(p-1)} \equiv 1 \mod p$ which is exactly the claim.

9. Find all positive integers n such that $\phi(n)$ is prime. Explain!

   Solution:

   Let p be a prime which divides n. We know that $(p-1) \mid \phi(n)$.

   If $p \geq 5$ then $\phi(n)$ is even and greater than or equal to 4 and is then not prime. Thus we can only have $n = 2^a 3^b$.

   If $a \geq 3$ we know that $\phi(2^b) = 2^{a-1}(2-1) = 2^{a-1} \mid \phi(n)$ which then tells us that $4 \mid \phi(n)$, a contradiction. Thus we can only have $a = 0, 1, 2$.

   If $b \geq 2$ we know that $\phi(3^b) = 3^{b-1}(3-1) = 3^{b-1}2 \mid \phi(n)$ which then tells us $6 \mid \phi(n)$, a contradiction. Thus we can only have $b = 0, 1$.

   Thus we could only have $n \in \left\{2^0 3^0, 2^1 3^0, 2^2 3^0, 2^0 3^1, 2^1 3^1, 2^2 3^1\right\} = \{1, 2, 4, 3, 6, 12\}$ and checking these shows that only $n = 4, 3, 6$ work.

10. Show that if a is relatively prime to m and $\text{ord}_m a = m - 1$ then m is prime.

    Solution:

    Given that $\text{ord}_m a = m - 1$, since $\text{ord}_m a \mid \phi(m)$ we have $m - 1 \mid \phi(m)$. But $\phi(m) \leq m - 1$ so then $\phi(m) = m - 1$ so then m is prime (since everything less than it is relatively prime to it.)