Discrete Structures

Modular Arithmetic Practice Problems

Name and ID: .....

1. Compute $(1001 \bmod d)$ for $d = 2, 3, \ldots, 10$.

Compute $(1001^2 \bmod d)$ for $d = 2, 3, \ldots, 10$.

2. Definition: m is the **inverse** of n modulo d if $(nm \bmod d) = 1$.

   Find the inverse of $n = 2, 3, \ldots, 10$ modulo 11 if exists. Explain how you found the inverses.

Find the inverse of $n = 2, 3, \ldots, 8$ modulo 9 if exists. Explain how you found the inverses.

3. Euler's Totient function: $\varphi(n)$ is the number of positive integers less than n that are relatively prime to n.

   Proposition: $\varphi(p) = p - 1$ for any prime number p.

   Proposition: $\varphi(p^k) = p^k - p^{k-1}$ for any positive integer k and a prime number p.

   Proposition: $\varphi(nm) = \varphi(n)\varphi(m)$ for any two relatively prime n and m ($\gcd(n, m) = 1$).

   Compute $\varphi(127)$. Justify your answer.

   Compute $\varphi(625)$. Justify your answer.

   Compute $\varphi(713)$. Justify your answer.

   Compute $\varphi(360)$. Justify your answer.

4. Compute (2^{100} mod 3), (2^{100} mod 5), and (2^{100} mod 7). Explain how you got the answers.

Compute (19^{90} mod 31). Explain how you got the answer.

Hint: use Fermat's Little Theorem.

Compute (47^{61} mod 77). Explain how you got the answer.

Hint: use Euler's Theorem.

5. Definition: $\gcd(n, m)$ is the largest positive integer that divides both n and m.

   Let $p \neq q$ be two different prime numbers. What is $\gcd(p, q)$? Justify your answer.

   Let k and h be two positive integers. What is $\gcd(2^k, 3^h)$? Justify your answer.

   Find $\gcd(1001, 4433)$ using the Euclid Algorithm. Show the execution of the algorithm.

   Find $\gcd(60, 84, 140)$. Justify your answer.

6. Definition: $\text{lcm}(n, m)$ is the least positive integer that is a multiple of both n and m.
   Justify your answers to the following four problems.
   Let $p \neq q$ be two different prime numbers. What is $\text{lcm}(p, q)$?

Find $\text{lcm}(35, 55, 65)$.

Find the smallest positive integer $n > 1$ for which $(n \bmod 10) = (n \bmod 14) = 1$.

Find the smallest positive integer $n > 1$ for which $(n \bmod d) = 1$ for **all** $2 \leq d \leq 10$.