Discrete Structures

Modular Arithmetic Practice Problems: solutions

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

$$\begin{aligned}
1001 = 500 \cdot 2 + 1 &\implies (1001 \bmod 2) = 1 \\
1001 = 333 \cdot 3 + 2 &\implies (1001 \bmod 3) = 2 \\
1001 = 250 \cdot 4 + 1 &\implies (1001 \bmod 4) = 1 \\
1001 = 200 \cdot 5 + 1 &\implies (1001 \bmod 5) = 1 \\
1001 = 166 \cdot 6 + 5 &\implies (1001 \bmod 6) = 5 \\
1001 = 143 \cdot 7 + 0 &\implies (1001 \bmod 7) = 0 \\
1001 = 125 \cdot 8 + 1 &\implies (1001 \bmod 8) = 1 \\
1001 = 111 \cdot 9 + 2 &\implies (1001 \bmod 9) = 2 \\
1001 = 100 \cdot 10 + 1 &\implies (1001 \bmod 10) = 1
\end{aligned}$$

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

$$\begin{aligned}
(1001^2 \bmod 2) &= ((1001 \bmod 2)^2 \bmod 2) = (1^2 \bmod 2) = 1 \\
(1001^2 \bmod 3) &= ((1001 \bmod 3)^2 \bmod 3) = (2^2 \bmod 3) = 1 \\
(1001^2 \bmod 4) &= ((1001 \bmod 4)^2 \bmod 4) = (1^2 \bmod 4) = 1 \\
(1001^2 \bmod 5) &= ((1001 \bmod 5)^2 \bmod 5) = (1^2 \bmod 5) = 1 \\
(1001^2 \bmod 6) &= ((1001 \bmod 6)^2 \bmod 6) = (5^2 \bmod 6) = 1 \\
(1001^2 \bmod 7) &= ((1001 \bmod 7)^2 \bmod 7) = (0^2 \bmod 7) = 0 \\
(1001^2 \bmod 8) &= ((1001 \bmod 8)^2 \bmod 8) = (1^2 \bmod 8) = 1 \\
(1001^2 \bmod 9) &= ((1001 \bmod 9)^2 \bmod 9) = (2^2 \bmod 9) = 4 \\
(1001^2 \bmod 10) &= ((1001 \bmod 10)^2 \bmod 10) = (1^2 \bmod 10) = 1
\end{aligned}$$

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.

$$
\begin{aligned}
2 \cdot 6 = 12 = 1 \cdot 11 + 1 &\quad \Longrightarrow \quad (2^{-1} \bmod 11) = 6 \\
3 \cdot 4 = 12 = 1 \cdot 11 + 1 &\quad \Longrightarrow \quad (3^{-1} \bmod 11) = 4 \\
4 \cdot 3 = 12 = 1 \cdot 11 + 1 &\quad \Longrightarrow \quad (4^{-1} \bmod 11) = 3 \\
5 \cdot 9 = 45 = 4 \cdot 11 + 1 &\quad \Longrightarrow \quad (5^{-1} \bmod 11) = 9 \\
6 \cdot 2 = 12 = 1 \cdot 11 + 1 &\quad \Longrightarrow \quad (6^{-1} \bmod 11) = 2 \\
7 \cdot 8 = 56 = 5 \cdot 11 + 1 &\quad \Longrightarrow \quad (7^{-1} \bmod 11) = 8 \\
8 \cdot 7 = 56 = 5 \cdot 11 + 1 &\quad \Longrightarrow \quad (8^{-1} \bmod 11) = 7 \\
9 \cdot 5 = 45 = 4 \cdot 11 + 1 &\quad \Longrightarrow \quad (9^{-1} \bmod 11) = 5 \\
10 \cdot 10 = 12 = 1 \cdot 11 + 1 &\quad \Longrightarrow \quad (10^{-1} \bmod 11) = 10
\end{aligned}
$$

   Find the inverse of $n = 2, 3, \ldots, 8$ modulo 9 if exists.

$$
\begin{aligned}
2 \cdot 5 = 10 = 1 \cdot 9 + 1 &\quad \Longrightarrow \quad (2^{-1} \bmod 9) = 5 \\
4 \cdot 7 = 28 = 3 \cdot 9 + 1 &\quad \Longrightarrow \quad (4^{-1} \bmod 9) = 7 \\
5 \cdot 2 = 10 = 1 \cdot 9 + 1 &\quad \Longrightarrow \quad (5^{-1} \bmod 9) = 2 \\
7 \cdot 4 = 28 = 3 \cdot 9 + 1 &\quad \Longrightarrow \quad (7^{-1} \bmod 9) = 4 \\
8 \cdot 8 = 64 = 7 \cdot 9 + 1 &\quad \Longrightarrow \quad (8^{-1} \bmod 9) = 8
\end{aligned}
$$

   - Both $(3n \bmod 9)$ and $(6n \bmod 9)$ are either $(0 \bmod 9)$ or $(3 \bmod 9)$ or $(6 \bmod 9)$ for any integer n. Therefore, neither 3 nor 6 have an inverse modulo 9.
   - In general, if $\gcd(n, d) \neq 1$ then n does not have an inverse modulo d. Therefore, since $\gcd(3, 9) = 3$ and $\gcd(6, 9) = 3$, it follows that both 3 and 6 do not have an inverse modulo 9.

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

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

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

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

   - 127 is a prime number. Therefore, by Proposition I,
   $$\begin{aligned}\varphi(127) &= 127 - 1 \\ &= 126\end{aligned}$$

   - $625 = 5^4$ and 5 is a prime number. Therefore, by Proposition II,
   $$\begin{aligned}\varphi(625) &= \varphi(5^4) \\ &= 5^4 - 5^3 \\ &= 625 - 125 \\ &= 500\end{aligned}$$

   - $713 = 31 \cdot 23$ and $\gcd(31, 23) = 1$ because both 31 and 23 are prime numbers. Therefore, by Propositions III and Proposition I,
   $$\begin{aligned}\varphi(713) &= \varphi(31 \cdot 23) \\ &= \varphi(31) \cdot \varphi(23) \\ &= (31 - 1)(23 - 1) \\ &= 30 \cdot 22 \\ &= 660\end{aligned}$$

   - $360 = 2^3 \cdot 3^2 \cdot 5$ and 2, 3, and 5 are prime numbers. Therefore, by Propositions I, II, and III,
   $$\begin{aligned}\varphi(360) &= \varphi(2^3 \cdot 3^2 \cdot 5) \\ &= \varphi(2^3) \cdot \varphi(3^2) \cdot \varphi(5) \\ &= (2^3 - 2^2) \cdot (3^2 - 3^1) \cdot 4 \\ &= 4 \cdot 6 \cdot 4 \\ &= 96\end{aligned}$$

4. Modular exponentiation.

- Since $2^{100} = (2^2)^{50} = 4^{50}$ and $(4 \bmod 3) = 1$, it follows that

$$\begin{aligned}(2^{100} \bmod 3) &= (4^{50} \bmod 3)\\ &= ((4 \bmod 3)^{50}) \bmod 3\\ &= (1^{50} \bmod 3)\\ &= (1 \bmod 3)\\ &= 1\end{aligned}$$

- Since $2^{100} = (2^4)^{25} = 16^{50}$ and $(16 \bmod 5) = 1$, it follows that

$$\begin{aligned}(2^{100} \bmod 5) &= (16^{25} \bmod 5)\\ &= ((16 \bmod 5)^{25}) \bmod 5\\ &= (1^{25} \bmod 5)\\ &= (1 \bmod 5)\\ &= 1\end{aligned}$$

- Since $2^{100} = 2 \cdot (2^3)^{33} = 2 \cdot 8^{33}$ and $(8 \bmod 7) = 1$, it follows that

$$\begin{aligned}(2^{100} \bmod 7) &= ((2 \cdot 8^{33}) \bmod 7)\\ &= ((2 \bmod 7) \cdot (8 \bmod 7)^{33}) \bmod 7\\ &= ((2 \cdot 1^{33}) \bmod 7)\\ &= (2 \bmod 7)\\ &= 2\end{aligned}$$

- 31 is a prime number, therefore $(19^{30} \bmod 31) = 1$ by Fermat's Little Theorem.

$$\begin{aligned}(19^{90} \bmod 31) &= ((19^{30})^3 \bmod 31)\\ &= ((19^{30} \bmod 31)^3 \bmod 31)\\ &= (1^3 \bmod 31)\\ &= (1 \bmod 31)\\ &= 1\end{aligned}$$

- $\gcd(47, 77) = 1$ and

$$\varphi(77) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$$

  Therefore, Euler's Theorem implies that $(47^{60} \bmod 77) = 1$.

$$\begin{aligned}(47^{61} \bmod 77) &= ((47 \cdot 47^{60}) \bmod 77)\\ &= (((47 \bmod 77) \cdot (47^{60} \bmod 77)) \bmod 77)\\ &= ((47 \cdot 1) \bmod 77)\\ &= (47 \bmod 77)\\ &= 47\end{aligned}$$

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 $\gcd(p, q)$?

  Answer: Let $g = \gcd(p, q)$. Since $g \mid p$ and $g \mid q$ and both p and q are prime numbers, it follows that the only candidates for the greatest common divisor of p and q are 1, p, and q. But $p \not| q$ and $q \not| p$. Therefore, $\gcd(p, q) = 1$.

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

  Answer: The only divisors of 2^k are powers of 2 and the only divisors of 3^h are powers of 3. As a result, 2^k and 3^h do not have a common divisor greater than 1. that is, $\gcd(2^k, 3^h) = 1$.

- Find $\gcd(1001, 4433)$ using the Euclid Algorithm.

  Answer: Euclid's algorithm finds the $\gcd(4433, 1001)$ in three rounds.

  (a) The pair $(4433, 1001)$ is replaced by the pair $(1001, 429)$ since $4433 = 4 \cdot 1001 + 429$.

  (b) The pair $(1001, 429)$ is replaced by the pair $(429, 143)$ since $1001 = 2 \cdot 429 + 143$.

  (c) The algorithm terminates because $429 = 3 \cdot 143$.

  Indeed, The prime factorizations of both numbers are

  $$\begin{aligned} 1001 &= 7 \cdot 11 \cdot 13 \\ 4433 &= 11 \cdot 13 \cdot 31 \end{aligned}$$

  Therefore, $\gcd(1001, 4433) = 11 \cdot 13 = 143$.

- Find $\gcd(60, 84, 140)$.

  Answer: The prime factors of the three numbers are

  $$\begin{aligned} 60 &= 2^2 \cdot 3 \cdot 5 \\ 84 &= 2^2 \cdot 3 \cdot 7 \\ 140 &= 2^2 \cdot 5 \cdot 7 \end{aligned}$$

  As a result, only $4 = 2^2$ divides all three numbers. Therefore, $\gcd(60, 84, 140) = 4$.

  Note that $\gcd(60, 84) = 12$, $\gcd(60, 140) = 20$, and $\gcd(84, 140) = 28$. But the greatest common divisor of all three numbers is only 4.

6. Definition: $\text{lcm}(n, m)$ is the least positive integer that is a multiple of both n and m.

- Let $p \neq q$ be two different prime numbers. What is $\text{lcm}(p, q)$?

  Answer: $\text{lcm}(p, q) = p \cdot q$.

  Proof I: Let $\ell = \text{lcm}(p, q)$. Since $p \mid \ell$ and $q \mid \ell$, it follows that $\ell = k \cdot p = h \cdot q$ for some integers k and h. Hence, $p \mid h \cdot q$. Since p and q are prime numbers, it must be the case that $p \mid h$. The smallest possible such h is $h = p$.

  Proposition: $n \cdot m = \text{lcm}(n, m) \cdot \text{gcd}(n, m)$ for any two integers n and m.

  Proof II: Both p and q are prime numbers and therefore $\text{gcd}(p, q) = 1$. The above proposition implies that

  $$\text{lcm}(p, q) = \frac{p \cdot q}{\text{gcd}(p, q)} = \frac{p \cdot q}{1} = p \cdot q$$

- What is $\text{lcm}(35, 55, 65)$?

  Answer: $35 = 5 \cdot 7$, $55 = 5 \cdot 11$, and $65 = 5 \cdot 13$. Therefore,

  $$\text{lcm}(35, 55, 65) = 5 \cdot 7 \cdot 11 \cdot 13 = 5005$$

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

  Answer: Both 10 and 14 must divide $n - 1$. Therefore, the smallest positive integer is $\text{lcm}(10, 14) + 1$. The answer is $n = 71$ since

  $$\text{lcm}(10, 14) = \text{lcm}(2 \cdot 5, 2 \cdot 7) = 2 \cdot 5 \cdot 7 = 70$$

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

  Answer: The nine integers $2, 3, \ldots, 10$ must divide $n - 1$. Therefore, the smallest positive integer is $\text{lcm}(2, 3, 4, 5, 6, 78, 9, 10) + 1$. The answer is $n = 2521$ since

  $$\begin{array}{lcll} \text{lcm}(2,3,4,5,6,7,8,9,10) & = & \text{lcm}(6,7,8,9,10) & (*\ 2,3,4,5 \text{ are divisors of } 6,8,10\ *) \\ & = & \text{lcm}(2 \cdot 3, 7, 2^3, 3^2, 2 \cdot 5) & (*\ \text{the prime factors of } 6,7,8,9,10\ *) \\ & = & 2^3 \cdot 3^2 \cdot 5 \cdot 7 & (*\ \text{the union of the prime factors}\ *) \\ & = & 2520 & \end{array}$$