Discrete Math Question Set 6

Abrar Habib

December 25, 2022

1. Assuming n ¿ 1, determine the values of the integer n for which the given congruence is true $28 \equiv 6 \pmod{n}$

   $28 = kn + 6$ for some integer k. We solve for k: $22 = kn \implies \frac{22}{k} = n$. If $k = 1, n = 22$. If $k = 2, n = 11$. If $k = 11, n = 2$. These are the only values of k that return an integer for n bigger than 1. The values of n are 2, 11, and 22.

2. List four elements in each of the following equivalence classes.

   (a) [1] in $\mathbb{Z}_7$

   x = 1 mod 7, x = 7k+1. The four elements are: 1,8,15,22.

   (b) [2] in $\mathbb{Z}_1 1$

   x = 2 mod 11. x = 11k+2. The four elements are 2,13,24,35.

   (c) [10] in $\mathbb{Z}_1 7$.

   x = 10 mod 17. x = 17k+10. The four elements are 10,27,44,61.

3. Determine whether or not the following set is a group under the stated binary operation. If so, determine its identity and the inverse of each of its elements. If it is not a group, state the condition(s) of the definitions that it violates.

   $\{a/2^n | a, n \in \mathbb{Z}, n \geq 0\}$ under addition

   Let $a, b \in \mathbb{Z}$ and $n, m \in \mathbb{Z}$, then $\frac{a}{2^n} + \frac{b}{2^m} = \frac{a2^m + b2^n}{2^{m+n}}$. Let $p = m + n$. Let $c = a2^m + b2^n$ Since $a, b, m, n \in \mathbb{Z}, c \in \mathbb{Z}$. $\frac{a2^m + b2^n}{2^{m+n}} = \frac{c}{2^p}$ This is closed under addition.

   Let $a, b, c \in \mathbb{Z}$ and $n, m, p \in \mathbb{Z}$ where $n, m, p > 0$.

   $\frac{a}{2^n} + (\frac{b}{2^m} + \frac{c}{2^p}) = \frac{a2^{m+p}b2^{n+p} + c2^{m+n}}{2^{m+p+n}}$.

   $(\frac{a}{2^n} + \frac{b}{2^m}) + \frac{c}{2^p} = \frac{a2^{m+p}b2^{n+p} + c2^{m+n}}{2^{m+p+n}}$.

   This shows addition is associative on this set.

   Let $e \{a/2^n | a, n \in \mathbb{Z}, n > 0\}$. $\frac{a}{2^n} + e = \frac{a}{2^n}.e = \frac{a}{2^n} - \frac{a}{2^n}.e = 0$. Identity 0, belongs to the set.

   $\frac{a}{2^n} + p = p + \frac{a}{2^n} = e$. $p = -\frac{a}{2^n}$. Since $a \in \mathbb{Z}$ and has inverse $(-a) \in \mathbb{Z}$, This set has an inverse.

   This set is a group with identity 0 and inverse $\frac{-a}{2^n}$.

4. Why is the set $\mathbb{Z}$ not a group under subtraction?

   Let $x = 1, y = 2, z = 3$. $(x - y) - z = (1 - 2) - 3 = -4. x - (y - z) = 1 - (2 - 3) = 1 - (-1) = 2$. Not a group under subtraction because it violates associative property.

5. Let $f : (\mathbb{Z} \times \mathbb{Z}, \oplus) \to (\mathbb{Z}, +)$ be the function defined by $f(x, y) = x - y$. [Here $(Z \times \mathbb{Z}, \oplus)$ has the binary operation $(a, b) \oplus (c, d) = (a + c, b + d)$ where $a + c$ and $b + d$ are computed using ordinary addition, and $(\mathbb{Z}, +)$ is the group of integers under ordinary addition.]

   (a) Prove that f is a homomorphism onto $\mathbb{Z}$.

   To show that f is a homomorphism, we must show that

   $f((a, b) \oplus (c, d)) = f((a, b)) + f((c, d))$.

$$\begin{aligned} f((a, b) \oplus (c, d)) &= f((a + c, b + d)) && (1) \\ &= a + c - (b + d) && (2) \\ &= a + c - b - d && (3) \\ &= a - b + c - d && (4) \\ &= f((a, b)) + f((c, d)). && (5) \end{aligned}$$

   f is a homomorphism.

   (b) Determine all $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ with $f(a, b) = 0$.

   $f(a, b) = a - b = 0 \implies a = b \implies a = b$.

   (c) Find $f^{-1}(7)$.

   We need to find (x,y) such that f(x,y) = 7. f(x,y) = x-y = 7. y = x-7.

   $f^{-1}(7) = \{x, x - 7 | x \in \mathbb{Z}\}$

   (d) If $E = \{2n | n \in \mathbb{Z}\}$, what is $f^{-1}(E)$?

   $f^{-1}(E)$ is the set of all (x,y) in $\mathbb{Z} \times \mathbb{Z}$.

   $f(x, y) = x - y = 2n.y = x - 2n$.

   $f^{-1}(E) = \{x, x - 2n | x, n \in \mathbb{Z}\}$

6. Determine the multiplicative inverse of the matrix

$$\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \tag{6}$$

   in the ring $M_2(\mathbb{Z})$ - that is, find a, b, c, d so that

$$\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{7}$$

   $\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix}^{-1} = \frac{1}{1*7-3*2} \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix}$.

   $a = 7, b = -2, c = -3, d = 1$

7. In question 6, show that

$$\begin{bmatrix} 1 & 2 \\ 3 & 8 \end{bmatrix} \tag{8}$$

is a unit in the ring $M_2(\mathbb{Q})$ but not a unit in $M_2(\mathbb{R})$.

$\begin{bmatrix} 1 & 2 \\ 3 & 8 \end{bmatrix}^{-1} = \frac{1}{1*8-3*2} \begin{bmatrix} 8 & -2 \\ -3 & 1 \end{bmatrix}.$

8. Verify that $(Z_{p,}^{*}.)$ is cyclic for the primes 5, 7, 11.

For p = 5, $Z_p^* = Z_5^* = 1, 2, 3, 4$. We can see that 2^1 mod $5 = 2, 2^2$ mod $5 = 4, 2^3$ mod $5 = 3, 2^4$ mod $5 = 1$

For p = 7, $Z_p^* = Z_7^* = 1, 2, 3, 4, 5, 6$. We can see that 3^1 mod $7 = 3, 3^2$ mod $7 = 2, 3^3$ mod $7 = 6, 3^4$ mod $7 = 4$ 3^5 mod $7 = 5, 3^6$ mod $7 = 1$.

For p = 11, $Z_p^* = Z_1^* = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$. We can see that 2^1 mod $11 = 2, 2^2$ mod $11 = 4, 2^3$ mod $11 = 8, 2^4$ mod $11 = 5$ 2^5 mod $11 = 10, 2^6$ mod $11 = 9, 2^7$ mod $11 = 7, 2^8$ mod $11 = 3, 2^9$ mod $11 = 6, 2^{10}$ mod $11 = 1$.

All of these are cyclic.

9. Determine whether or not the following set of numbers is a ring under ordinary addition and multiplication.

$$R = a + b\sqrt{2} + c\sqrt{3} | a \in \mathbb{Z}, b, c \in \mathbb{Q}$$

Let $a = 1, b = \frac{1}{2}, a_2 = 1, b_2 = \frac{1}{3}$. Allow c to be 0.

$a + b\sqrt{2} + 0\sqrt{3} \cdot a_2 + b_2\sqrt{2} + 0\sqrt{3} = (1 + \frac{\sqrt{2}}{2}) \cdot (1 + \frac{sqrt2}{3}) \implies 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{3} + \frac{2}{3}$. This result is not part of $\mathbb{Z}$. Therefore R is not a ring.

10. If R is a ring with unity and a, b are units of R, prove that ab is a unit of R and that $(ab)^{-1} = b^{-1}a^{-1}$.

$ab \cdot (ab)^{-1} = 1 \implies ab \cdot b^{-1}a^{-1} \implies abb^{-1}a^{-1}. \implies a(bb^{-1})a^{-}1 \implies a(1) \cdot a^{-1} \implies a \cdot a^{-1} = 1$ ab is a unit of R.

Prove $(ab)^{-1} = b^{-1}a^{-1}$:

$$abb^{-1}a^{-1} = (ab)(ab)^{-1} \tag{9}$$
$$(ab) \cdot (b^{-1}a^{-1}) = (ab)(ab)^{-1} \tag{10}$$
$$(b^{-1}a^{-1}) = (ab)^{-1} \tag{11}$$

11. Prove that a unit in a ring R cannot be a proper divisor of zero.

Let $x \in \mathbb{R}$. There exists a $y \in \mathbb{R}$ such that $x \cdot y = y \cdot x = 1$. Suppose $x \cdot w = z$ for some $w \in \mathbb{R}$. Where z is the addition identity. $y \cdot (x \cdot w) = y \cdot z = z$. $(y \cdot x) \cdot w = 1 \cdot w = w$.

12. For $a, b \in \mathbb{Z}+$ and $s, t \in \mathbb{Z}$ what can we say about gcd(a,b) if $as + bt = 4$?

    gcd(a,b) will either be 1, 2, or 4 since those are the divisor of 4.

13. Use the Euclidean algorithm to express gcd(26, 91) as a linear combination of 26 and 91.

    $26 = 3 \cdot 91 + 26 \implies 91 = 3 \cdot 26 + 13 \implies 26 = 2 \cdot 13 + 0 \implies gcd(26, 91) = 13.$

14. Are these statements true or false? Explain the reason briefly.

    (a) The sum of any three consecutive integers is divisible by 3.

    True. Three consecutive integers $x, x + 1, x + 2$ add up to $(3x + 3)$ which if you factor into $3(x + 1)$ is divisible by 3.

    (b) The product of any two even integers is a multiple of 4.

    Let x and y be even integers. $xy = 2x \cdot 2y = 4(x + y)$. Therefore the product of any two even integers is a multiple of 4.