Solutions Resit Exam: Numbers 2025

0. Let $a_n = (3^{2n} - 8n - 1)/64$. Show that $a_n \in \mathbb{Z}$ for all integers n.

   Solution: We must show $3^{2n} - 8n - 1 \equiv 0 \pmod{64}$. We proceed by induction.

   Base case ($n = 0$): $3^0 - 0 - 1 = 1 - 1 = 0$. 0 is divisible by 64.

   Inductive step: Assume $3^{2k} - 8k - 1 = 64m$ for some integer m.

   Consider $n = k + 1$:

   $$3^{2(k+1)} - 8(k+1) - 1 = 9 \cdot 3^{2k} - 8k - 9 = 64(9m + k)$$

   Since $9m + k$ is an integer, the expression is divisible by 64. Thus $a_n \in \mathbb{Z}$.

1. Prove that, if a and b are relatively prime, then $\gcd(2a + b, a + 2b) =$ 1 or 3.

   Solution: Let $d = \gcd(2a + b, a + 2b)$. Then d divides any linear combination of these terms.

   $$d \mid 2(a + 2b) - (2a + b) = 2a + 4b - 2a - b = 3b$$
   $$d \mid 2(2a + b) - (a + 2b) = 4a + 2b - a - 2b = 3a$$

   Thus d divides $\gcd(3a, 3b) = 3\gcd(a, b)$. Since $\gcd(a, b) = 1$, we have $d \mid 3$. So the GCD is either 1 or 3.

2. *Prove or disprove.* If $a^3 \mid c^2$ then $a \mid c$.

   Solution: Let the prime factorization of a be $\prod p_i^{\alpha_i}$ and c be $\prod p_i^{\gamma_i}$. $a^3 \mid c^2$ implies that for every prime factor p_i, the exponent in a^3 is less than or equal to the exponent in c^2:

   $$3\alpha_i \leq 2\gamma_i$$

   We need to prove $a \mid c$, which requires $\alpha_i \leq \gamma_i$. Since $\alpha_i \geq 1$ (if $\alpha_i = 0$ it's trivial), we divide the inequality by 2:

   $$\frac{3}{2}\alpha_i \leq \gamma_i$$

Since $\alpha_i < \frac{3}{2}\alpha_i$, it follows that $\alpha_i < \gamma_i$. Thus $\alpha_i \leq \gamma_i$ holds. Therefore, $a \mid c$.

3. a) For which values of k does $315x + 56y = k$ have integer solutions?

   Solution: We calculate $d = \gcd(315, 56)$ using the Euclidean Algorithm:

$$\begin{aligned} 315 &= 5 \times 56 + 35 \\ 56 &= 1 \times 35 + 21 \\ 35 &= 1 \times 21 + 14 \\ 21 &= 1 \times 14 + 7 \\ 14 &= 2 \times 7 + 0 \end{aligned}$$

   The last non-zero remainder is 7, so $\gcd(315, 56) = 7$. Therefore, solutions exist if and only if $7 \mid k$ (i.e., k is a multiple of 7).

   b) Solve $315x \equiv 24 \pmod{56}$.

   Solution: This is equivalent to solving $315x + 56y = 24$. As found in (a), the GCD is 7. For a solution to exist, 7 must divide 24. Since 7 does not divide 24, no solutions exist.

4. Prove that $437 = 19 \cdot 23$ divides $3^{396} - 1$.

   Solution: We check modulo 19 and modulo 23 separately.

   Mod 19: By Fermat's Little Theorem (FLT), $3^{18} \equiv 1 \pmod{19}$. Note that $396 = 18 \times 22$.

$$3^{396} = (3^{18})^{22} \equiv 1^{22} \equiv 1 \pmod{19}$$

   So $19 \mid 3^{396} - 1$.

   Mod 23: By FLT, $3^{22} \equiv 1 \pmod{23}$. Note that $396 = 22 \times 18$.

$$3^{396} = (3^{22})^{18} \equiv 1^{18} \equiv 1 \pmod{23}$$

   So $23 \mid 3^{396} - 1$.

   Since $\gcd(19, 23) = 1$, their product 437 divides $3^{396} - 1$.

5. Show that if a and n are not relatively prime, then a has no multiplicative inverse modulo n.

   Solution: Assume for the sake of contradiction that a has an inverse x modulo n. Then $ax \equiv 1 \pmod{n}$, which means $ax - ny = 1$ for some integer y.

   Let $d = \gcd(a, n)$. Since they are not relatively prime, $d > 1$. Since $d \mid a$ and $d \mid n$, d must divide any linear combination of a and n. Thus $d \mid (ax - ny)$, so $d \mid 1$. This implies $d = 1$, which contradicts $d > 1$. Therefore, no inverse exists.

6. *Prove or disprove.* The matrix equation over $\mathbb{Z}/35\mathbb{Z}$ has a unique solution.

   Solution: Let $A = \begin{pmatrix} \bar{3} & \bar{2} \\ \bar{7} & \bar{6} \end{pmatrix}$. This matrix has a unique solution (is invertible) if and only if its determinant is a unit (invertible) in $\mathbb{Z}/35\mathbb{Z}$. We calculate the determinant:

   $$\det(A) = (\bar{3})(\bar{6}) - (\bar{2})(\bar{7}) = \bar{4}.$$

   As $\gcd(4, 35) = 1$, 4 has a multiplicative inverse. Therefore, A^{-1} exists and is unique.

7. Show that $1^p + 2^p + \ldots + (p-1)^p \equiv 0 \pmod{p}$ when p is an odd prime.

   Solution: By Fermat's Little Theorem, for any integer a, $a^p \equiv a \pmod{p}$ as $a \in \{1, 2, \ldots, p-1\}$ satisfies $\gcd(a, p) = 1$. Thus, the sum becomes:

   $$S \equiv 1 + 2 + 3 + \cdots + (p-1) \pmod{p}$$

   Using the formula for the sum of the first n integers:

   $$S \equiv \frac{(p-1)p}{2} \pmod{p}$$

   Since p is an odd prime, $p - 1$ is even, so $\frac{p-1}{2}$ is an integer, say k.

   $$S \equiv k \cdot p \equiv 0 \pmod{p}$$

8. Find four positive integers n such that $\varphi(n) = 24$.

   Solution: Possible values:

   (a) $n = 35$: $\varphi(35) = \varphi(5)\varphi(7) = 4 \times 6 = 24$.

   (b) $n = 39$: $\varphi(39) = \varphi(3)\varphi(13) = 2 \times 12 = 24$.

   (c) $n = 45$: $\varphi(45) = \varphi(9)\varphi(5) = (3^2 - 3^1)(4) = 6 \times 4 = 24$.

   (d) $n = 56$: $\varphi(56) = \varphi(8)\varphi(7) = (2^3 - 2^2)(6) = 4 \times 6 = 24$.

   Other examples: 52, 70, 72, 84.