

**Listado 02: Aritmética modular
Teoría de Números (527288)**

1. Justificar: si la multiplicación por k es una biyección de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ en sí mismo, entonces k es invertible módulo n .
2. Justificar: si k es invertible módulo n , entonces la multiplicación por k es una biyección de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ en sí mismo.
3. Reduciendo cada una de las siguientes ecuaciones a módulos apropiados, mostrar que no tienen soluciones enteras:
 - a) $x^4 - 3x + 10 = 0$
 - b) $x^5 - x^2 + x - 3 = 0$
4. Simplificar las siguientes expresiones:
 - a) $(2+x)^5$ (mód 5)
 - b) 3^{1000} (mód 7)
 - c) 99^{999} (mód 100)
 - d) $1 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot \dots \cdot 999 \cdot 1001$ (mód 8)
5. Determinar:
 - a) las soluciones módulo 15 de $x \equiv 2$ (mód 5);
 - b) las soluciones módulo 16 de $x \equiv 1$ (mód 8);
 - c) las soluciones módulo 120 de $x \equiv 5$ (mód 6).
6. En el documento Ecuaciones mod n:
 - a) en el apartado **Ecuaciones lineales**, verificar que los casos señalados son los únicos posibles;
 - b) en el apartado **Ecuaciones lineales**, demostrar las conclusiones de cada caso;
 - c) en el apartado **Teorema Chino**, demostrar las cuatro igualdades señaladas y utilizarlas para verificar que la solución indicada es correcta.
7. Resolver las siguientes ecuaciones:
 - a) $2x \equiv 4$ (mód 6)
 - b) $12x \equiv 18$ (mód 36)
 - c) $5x \equiv 17$ (mód 21)
 - d) $x^2 \equiv 1$ (mód 35)
 - e) $x^3 \equiv 1$ (mód 21)
 - f) $x^2 - 4x \equiv 0$ (mód 21)
 - g) $49x \equiv 169$ (mód 60)
 - h) $x^4 - x^2 + 3 \equiv 0$ (mód 27)
8. Sabiendo que $x \equiv 3$ (mód 5) es la única solución de $x^5 - x^3 + 5x - 1 \equiv 0$ (mód 5), resolver
$$x^5 - x^3 + 5x - 1 \equiv 0 \pmod{5^4}$$
utilizando el Lema de Hensel.

Mini-proyecto: criterios de divisibilidad

Para estos criterios, recordar la escritura posicional decimal de los números naturales: el valor de cada dígito debe ser amplificado por una potencia de diez apropiada para reconstruir el valor de un número a partir de sus dígitos.

9. Justificar el criterio de divisibilidad por 2: un número es divisible por 2 si y sólo si su último dígito lo es.
10. Justificar el criterio de divisibilidad por 3: un número es divisible por 3 si y sólo si la suma de sus dígitos lo es.
11. Justificar el criterio de divisibilidad por 4: un número es divisible por 4 si y sólo si sus dos últimos dígitos forman un múltiplo de 4.
12. Justificar el criterio de divisibilidad por 5: un número es divisible por 5 si y sólo si su último dígito lo es.
13. Justificar el criterio de divisibilidad por 6: un número es divisible por 6 si y sólo si es divisible por 2 y por 3.
14. Justificar el criterio de divisibilidad por 7: un número es divisible por 7 si y sólo si el número siguiente lo es: tomar el número original, removerle el último dígito, multiplicar dicho dígito por dos, y restarlo del número al que se le quitó el dígito. Por ejemplo, 2387 es divisible por 7 pues $238 - 14 = 224$ lo es, pues $22 - 8 = 14$ lo es (aplicando el criterio dos veces).
15. Justificar el criterio de divisibilidad por 8: un número es divisible por 8 si y sólo si sus tres últimos dígitos forman un múltiplo de 8.
16. Justificar el criterio de divisibilidad por 9: un número es divisible por 9 si y sólo si la suma de sus dígitos lo es.
17. Justificar el criterio de divisibilidad por 10: un número es divisible por 6 si y sólo si su último dígito es cero.
18. Justificar el criterio de divisibilidad por 11: un número es divisible por 11 si y sólo si la suma de sus dígitos con signos alternados lo es. Por ejemplo, 707498 es divisible por 11 pues $7 - 0 + 7 - 4 + 9 - 8 = 11$ lo es.
19. Justificar el criterio de divisibilidad por 12: un número es divisible por 12 si y sólo si es divisible por 4 y por 3.
20. Inventar un criterio de divisibilidad por 13. (*Sugerencia: inspirarse en el de divisibilidad por 7.*)