Tarea IV de Álgebra Superior II

Semestre 2020-II

7 de mayo de 2020

Profra: Gabriela Campero Arena Ayud: Carlos Ochoa y Mariana Garduño

1. Demuestre las siguientes afirmaciones:

   (i) $\forall n \in \mathbb{Z}^+ \forall a, b \in \mathbb{Z}(a \equiv b \ (mod\ n) \Leftrightarrow \forall c \in \mathbb{Z}\,(a + c \equiv b + c \ (mod\ n)))$;

   (ii) $\forall n \in \mathbb{Z}^+ \forall a, b \in \mathbb{Z}(a \equiv b \ (mod\ n) \Leftrightarrow \forall c \in \mathbb{Z}\,(a - c \equiv b - c \ (mod\ n)))$;

   (iii) $\forall n \in \mathbb{Z}^+ \forall a, b \in \mathbb{Z}(a \equiv b \ (mod\ n) \Rightarrow \forall c \in \mathbb{Z}\,(a \cdot c \equiv b \cdot c \ (mod\ n)))$;

   (iv) $\forall n \in \mathbb{Z}^+ \forall a, b, c \in \mathbb{Z}((a \cdot c \equiv b \cdot c \ (mod\ n) \wedge (n; c) = 1) \Rightarrow (a \equiv b \ (mod\ n)))$;

   (v) para toda $n \in \mathbb{Z}^+$ y para cualesquiera $a, b \in \mathbb{Z}$, si $a = nq_1 + r_1$ con $0 \leq r_1 < n$ y $b = nq_2 + r_2$ con $0 \leq r_2 < n$, entonces $a \equiv b \ (mod\ n)$ si y sólo si $r_1 = r_2$;

   (vi) para toda $n \in \mathbb{Z}^+$, $\mathbb{Z}_n = \{[0]_n, [1]_n, ..., [n-1]_n\}$;

   (vii) $\forall n \in \mathbb{Z}^+ \forall a, b \in \mathbb{Z}(a \equiv b \ (mod\ n) \Rightarrow (a; n) = (b; n))$;

   (viii) $\forall n \in \mathbb{Z}^+ \forall a, b, c, d \in \mathbb{Z}((a \equiv b \ (mod\ n) \wedge c \equiv d \ (mod\ n)) \Rightarrow a + c \equiv b + d \ (mod\ n)))$;

   (ix) $\forall n \in \mathbb{Z}^+ \forall a, b, c, d \in \mathbb{Z}((a \equiv b \ (mod\ n) \wedge c \equiv d \ (mod\ n)) \Rightarrow a - c \equiv b - d \ (mod\ n)))$;

   (x) $\forall n \in \mathbb{Z}^+ \forall a, b, c, d \in \mathbb{Z}((a \equiv b \ (mod\ n) \wedge c \equiv d \ (mod\ n)) \Rightarrow ac \equiv bd \ (mod\ n)))$;

   (xi) $\forall n \in \mathbb{Z}^+ \forall a, b \in \mathbb{Z}(a \equiv b \ (mod\ n) \Leftrightarrow \forall m \in \mathbb{N}\,(a^m \equiv b^m \ (mod\ n)))$;

   (xii) $\forall n \in \mathbb{Z}^+ \forall a, b \in \mathbb{Z} \forall c \in \mathbb{Z}^+(a \equiv b \ (mod\ n) \Rightarrow a \cdot c \equiv b \cdot c \ (mod\ cn))$;

   (xiii) $\forall n \in \mathbb{Z}^+ \forall a, b \in \mathbb{Z} \forall c \in \mathbb{Z}^+((a \equiv b \ (mod\ n) \wedge c \mid n) \Rightarrow a \equiv b \ (mod\ c))$;

   (xiv) $\forall n \in \mathbb{Z}^+ \forall a, b \in \mathbb{Z} \forall c \in \mathbb{Z}^+((a \equiv b \ (mod\ n) \wedge c \mid a \wedge c \mid b \wedge c \mid n) \Rightarrow \frac{a}{c} \equiv \frac{b}{c} \ (mod\ \frac{n}{c}))$;

   (xv) $\forall a, n \in \mathbb{Z}\left(\frac{a}{(a;n)}; \frac{n}{(a;n)}\right) = 1$;

   (xvi) $\forall n \in \mathbb{Z}^+ \forall a, b, c \in \mathbb{Z}(ca \equiv cb \ (mod\ n) \Rightarrow a \equiv b \ (mod\ \frac{n}{(c;n)}))$;

   (xvii) $\forall n_1, n_2 \in \mathbb{Z}^+ \forall a, b, c, d \in \mathbb{Z}((a \equiv b \ (mod\ n_1) \wedge c \equiv d \ (mod\ n_2))$
   $\Rightarrow a + c \equiv b + d \ (mod\ (n_1; n_2)))$;

   (xviii) $\forall n_1, n_2 \in \mathbb{Z}^+ \forall a, b, c, d \in \mathbb{Z}((a \equiv b \ (mod\ n_1) \wedge c \equiv d \ (mod\ n_2))$
   $\Rightarrow ac \equiv bd \ (mod\ (n_1; n_2)))$.

2. Dé un contraejemplo de las siguientes afirmaciones:

   (i) $\forall n \in \mathbb{Z}^+ \setminus \{1\} \forall a, b, c \in \mathbb{Z}(a \cdot c \equiv b \cdot c \ (mod\ n) \implies (a \equiv b \ (mod\ n)))$, *sugerencia:* analice el inciso (iv) del ejercicio anterior;

   (ii) $\forall n \in \mathbb{Z}^+ \forall a, b \in \mathbb{Z}((a; n) = (b; n) \Rightarrow a \equiv b \ (mod\ n))$, compare con el inciso (vii) del ejercicio anterior;

   (iii) los "regresos" de los incisos (viii), (ix) y (x) del ejercicio anterior.

3. Demuestre las siguientes afirmaciones:

   (i) para toda $n \in \mathbb{Z}^+$, la definición de las operaciones de suma y multiplicación en $\mathbb{Z}_n$ están bien definidas (esdecir, no dependen de los representantes);

   (ii) para toda $n \in \mathbb{Z}^+$, $(\mathbb{Z}_n, +, \cdot)$ es un anillo conmutativo con unitario, donde $[0]_n$ es el neutro aditivo y $[1]_n$ es el unitario;

   (iii) para toda $n \in \mathbb{Z}^+$, $[a]_n$ es una unidad de $\mathbb{Z}_n$ si y sólo si $(a; n) = 1$.

4. Escriba las tablas de las operaciones de suma y multiplicación para $\mathbb{Z}_4$, $\mathbb{Z}_6$ y $\mathbb{Z}_7$ e identifique las unidades en todos ellos. Compare con el inciso (iii) del ejercicio anterior y diga qué se cumple en $\mathbb{Z}_7$ que no se cumple ni en $\mathbb{Z}_4$ ni en $\mathbb{Z}_6$ al respecto de las unidades y diga por qué.

5. Diga para cuáles enteros m se cumplen las siguientes afirmaciones, justificando su respuesta:

(i) $m \in \mathbb{Z}^+$ y $[1]_m$ es una unidad en $\mathbb{Z}_m$;
(ii) $m \in \mathbb{Z}^+$ y $[5]_m$ es una unidad en $\mathbb{Z}_m$;
(iii) $[m]_5$ es una unidad en $\mathbb{Z}_5$;
(iv) $[m]_{18}$ es una unidad en $\mathbb{Z}_{18}$;
(v) $m \in \mathbb{Z}^+$ y $27 \equiv 5 \ (mod\ m)$;
(vi) $m \in \mathbb{Z}^+$ y $1000 \equiv 1 \ (mod\ m)$;
(vii) $m \in \mathbb{Z}^+$ y $1331 \equiv 0 \ (mod\ m)$;
(viii) $m \in \mathbb{Z}^+$ y $[a]_m$ es una unidad en $\mathbb{Z}_m$ para todo $a \not\equiv 0 \ (mod\ m)$.

6. Sea $n \geq 2$. Denotamos con $\lfloor \sqrt{n} \rfloor$ al máximo entero z tal que $z \cdot z \leq n$. Demuestre que n es primo si y sólo si para cualquier m tal que $2 \leq m \leq \lfloor \sqrt{n} \rfloor$ se tiene que $m \not| n$.

7. Demuestre las siguientes afirmaciones:

   (i) para cualesquiera $n \in \mathbb{Z}^+$ y $a, b \in \mathbb{Z}$, la congruencia $ax \equiv b \ (mod\ n)$ tiene solución si y sólo si $(a; n) \mid b$;

   (ii) para cualesquiera $n \in \mathbb{Z}^+$ y $a, b \in \mathbb{Z}$, si $(a; n) \mid b$, entonces la congruencia $ax \equiv b \ (mod\ n)$ tiene exactamente $(a; n)$ soluciones incongruentes módulo n y éstas son:

$$x = \left(\frac{b}{(a;n)}\right) t + \left(\frac{n}{(a;n)}\right) k$$

   con $k \in \{0, 1, ..., (a; n) - 1\}$, donde t es tal que $[t]_{\frac{n}{(a;n)}}$ es un inverso de $[\frac{a}{(a;n)}]_{\frac{n}{(a;n)}}$ en $\mathbb{Z}_{\frac{n}{(a;n)}}$.

8. Diga si las siguientes ecuaciones tienen solución, justificando su respuesta, y si sí tienen solución dé todas las soluciones incongruentes según el módulo, justifique que lo son y que no hay ninguna otra incongruente a ellas:

   (i) $2x \equiv 5 \ (mod\ 7)$;
   (ii) $3x \equiv 6 \ (mod\ 9)$;
   (iii) $8x \equiv 14 \ (mod\ 24)$;
   (iv) $57x \equiv 208 \ (mod\ 4)$;
   (v) $362x \equiv 236 \ (mod\ 24)$;
   (vi) $12345x \equiv 111 \ (mod\ 6)$;
   (vii) $980x \equiv 1500 \ (mod\ 1600)$;
   (viii) $128x \equiv 833 \ (mod\ 1001)$;
   (ix) $6789783x \equiv 2474010 \ (mod\ 28927591)$.

9. Encuentre todas las soluciones positivas mínimas incongruentes según el módulo:

   (i) $13x \equiv 9 \ (mod\ 25)$.
   (ii) $207x \equiv 6 \ (mod\ 18)$.
   (iii) $259x \equiv 5 \ (mod\ 11)$.
   (iv) $7x \equiv 5 \ (mod\ 256)$.
   (v) $222x \equiv 12 \ (mod\ 18)$.

10. Encuentre todas las soluciones de
    $(3n - 2)x + 5n \equiv 0 \ (mod\ 9n - 9)$ con $n \geq 2$.

11. ¿Para cuáles enteros c con $0 \leq c < 30$ la congruencia $12x \equiv c \ (mod\ 30)$ tiene solución? En el caso en el que haya solución, ¿cuántas soluciones incongruentes hay?

12. Demuestre que para cualesquiera $a, b \in \mathbb{Z}$, si p es primo y $p \nmid a$, entonces la congruencia $ax \equiv b \ (mod\ p)$ tiene solución y todas las soluciones son congruentes módulo p (es decir, tiene una única solución módulo p).

13. (i) Diga si para los siguientes elementos de $\mathbb{Z}_{13}$ existe un inverso multiplicativo módulo 13 y si sí existe, encuéntrelo:

    (a) $[2]_{13}$ (b) $[15]_{13}$ (c) $[3]_{13}$ (d) $[11]_{13}$

    (ii) Diga si para los siguientes elementos de $\mathbb{Z}_{12}$ existe un inverso multiplicativo módulo 12 y si sí existe, encuéntrelo:

    (a) $[2]_{12}$ (b) $[16]_{12}$ (c) $[5]_{12}$ (d) $[11]_{12}$

    (iii) Demuestre que si $[c]_m$ es un inverso multiplicativo de $[a]_m$ en $\mathbb{Z}_m$ y $[d]_m$ es un inverso multiplicativo de $[b]_m$ en $\mathbb{Z}_m$, entonces $[c]_m[d]_m$ es un inverso multiplicativo de $[a]_m[b]_m$ en $\mathbb{Z}_m$.

    (iv) Determine las unidades de $\mathbb{Z}_m$.

14. Demuestre que $\mathbb{Z}_p$ es un dominio entero si y sólo si p es primo.

15. Demuestre que si p es primo, entonces $\mathbb{Z}_p$ es un campo.

16. Demuestre lo siguiente:

    (i) Todo entero es congruente módulo 7 con algún número del siguiente conjunto:

    $$\{191, 7, 54, 31, 36, 20, 767\}$$

    (ii) Un número natural es divisible entre 3 (resp. 9) si y sólo si la suma de sus dígitos es divisible entre 3 (resp. 9). (*sugerencia:* $n = r_k 10^k + r_{k-1}10^{k-1} + \cdots + r_2 10^2 + r_1 10^1$).

    (iii) Todo primo mayor que 5 es de la forma $30m + n$ con $n \in \{1, 7, 11, 13, 17, 19, 23, 29\}$.

    (iv) Si q es un primo y $q \neq 3$, en el conjunto $\{q, q+2, q+4\}$ siempre existe un número que es múltiplo de 3.

    (v) $1^5 + 2^5 + 3^5 + \ldots 11^5$ es múltiplo de 3 (*sugerencia:* use el inciso (xi) del 1).

    (vi) Si a es par, entonces $a^2 \equiv 0 (mod\ 4)$; y si a es impar, entonces $a^2 \equiv 1 (mod\ 4)$.

17. Muestre un sistema completo de residuos módulo 17 compuesto sólo por múltiplos de 3.

18. Encuentre el residuo de las siguientes divisiones (*sugerencia:* use incisos del ejercicio 1):

    (i) $1^5 + 2^5 + 3^5 + \ldots 11^5$ dividido entre 7.

    (ii) $1^5 + 2^5 + \cdots + 1080^5$ dividido entre 14

    (iii) $1! + 2! + 3! + \ldots (10^{10})!$ dividido entre 24.

    (iv) $\binom{3}{3} + \binom{4}{3} + \binom{5}{3} + \ldots + \binom{102}{3}$ dividido entre 7.

19. Encuentra los dos números positivos más pequeños que dejan residuo 2,3,2 al dividirlos entre 3,5,7 respectivamente.

20. Evalúe $\phi(m)$ para $m = 1, 2, ...12$.

21. Encuentre el menor entero positivo x que resuelva cada una de las siguientes congruencias (*sugerencia:* inciso (v) del ejercicio 1):

    (i) $572^{24} \equiv x (mod\ 4)$

    (ii) $321^{210} \equiv x (mod\ 5)$

    (iii) $232^{15} \equiv x (mod\ 10)$

    (iv) $3^{100} \equiv x (mod\ 5)$

    (v) $2^{21} \equiv x (mod\ 11)$.

22. Revise las demostraciones de todas las variantes del Teorema chino del residuo.

23. Diga cuáles de los siguientes sistemas de ecuaciones tienen solución, justificando su respuesta y si sí tienen solución, resuélvalos:

    (i)
    $$\begin{aligned} x &\equiv 1\ (mod\ 5) \\ x &\equiv 2\ (mod\ 6) \\ x &\equiv 3\ (mod\ 7) \end{aligned}$$

    (ii)
    $$\begin{aligned} x &\equiv 1\ (mod\ 2) \\ x &\equiv 2\ (mod\ 3) \\ x &\equiv 3\ (mod\ 5) \end{aligned}$$

    (iii)
    $$\begin{aligned} 5x &\equiv 1\ (mod\ 7) \\ 22x &\equiv 2\ (mod\ 6) \end{aligned}$$

    (iv)
    $$\begin{aligned} 8x &\equiv 14\ (mod\ 24) \\ 4x &\equiv 1\ (mod\ 125) \end{aligned}$$

    (v)
    $$\begin{aligned} 3^8 x &\equiv 3\ (mod\ 12) \\ 50x &\equiv 75\ (mod\ 125) \\ x &\equiv 1000\ (mod\ 91) \end{aligned}$$

    (vi)
    $$\begin{aligned} 2^{33} x &\equiv 10\ (mod\ 12) \\ 73x &\equiv 1\ (mod\ 219) \\ 12x &\equiv 4\ (mod\ 8) \end{aligned}$$

24. Resuelva los siguientes ejercicios, justificando sus respuestas:

    (i) Diga qué hora indica en este momento un reloj de manecillas si:

    (a) dentro de 29 horas marcará las 11 horas,

    (b) dentro de 100 horas marcará las 2,

    (c) hace 50 horas marcaba las 6.

(ii) Un astrónomo sabe que un satélite orbita la Tierra en un período que es un múltiplo exacto de una hora y que es menor que un día. Si el astrónomo observa que el satélite completa 11 órbitas en un intervalo de tiempo que comienza cuando un reloj (de 24 horas) marca las 0 horas de un día dado y termina cuando el reloj marca las 17 horas de otro día. ¿Cuánto dura el período de órbita del satélite?

(iii) Un grupo de 17 monos almacena sus plátanos en 11 pilas de igual medida y una doceava con 6 plátanos. Cuando ellos dividen los plátanos en 17 pilas no sobra ninguno, ¿cuál es el menor número de plátanos que pueden tener?

(iv) Los hombres de cierto ejército no podían ser divididos en grupos de 2, 3, 4,..., o 12, pues en cada caso sobraba un hombre; sin embargo, sí era posible dividirlos en 13 sin que sobrara ningún hombre. ¿Cuál es el menor número posible de hombres en el ejército? *Sugerencia:* Demuestre que si $x \equiv a \ (mod\ n)$ y $x \equiv a \ (mod\ m)$, entonces $x \equiv a \ (mod\ [n;m])$ y después generalícelo a que si $x \equiv a \ (mod\ m_1)$,..., y $x \equiv a \ (mod\ m_k)$, entonces $x \equiv a \ (mod\ [m_1;...;m_k])$.

(v) Una tienda vende una silla a un precio menor que el usual, que es de 99 pesos. Si venden un monto de 8137 pesos de éstas sillas y el descuento en el precio es un entero, ¿cuántas sillas vendieron?

(vi) Una banda de 17 ladrones roba un gran saco de billetes de 100 pesos. Tratan de reaprtir los billetes equitativamente, pero sobran 3 billetes. Dos de los ladrones empiezan a pelear por el sobrante hasta que uno le dispara al otro. Los billetes se redistribuyen, pero esta vez sobran 10 billetes. De nuevo empieza una pelea y otro ladrón resulta muerto. Cuando el dinero se redistribuye equitativamente, no sobra ninguno. ¿Cuál es el menor número posible de billetes que los ladrones robaron?

(vii) La producción diaria de huevos en una granja es inferior a 75. Al final de cierto día el recolector informa que la cantidad de huevos recogida es tal que contada de tres en tres sobran 2, contada de cinco en cinco sobran 4, y contada de siete en siete sobran 5. El capataz dice que no es posible. ¿Quién tiene la razón?