Tarea III de Álgebra Superior II

Semestre 2020-II

26 de marzo de 2020

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

1. Demuestre las siguientes afirmaciones:
   (i) $\forall a \in \mathbb{Z}(a \mid 0)$
   (ii) $\forall a \in \mathbb{Z}(0 \mid a \Leftrightarrow a = 0)$
   (iii) $\forall a \in \mathbb{Z}(a \mid a)$
   (iv) $\forall a, b, c \in \mathbb{Z}(a \mid b \wedge b \mid c \Rightarrow a \mid c)$
   (v) $\forall a, b \in \mathbb{Z}(a \mid b \Leftrightarrow |a| \mid |b|)$
   (vi) Si $a, b \in \mathbb{Z}$, $a \mid b$ y $b \mid a$, entonces $a = b \cdot u$ para alguna unidad u de $\mathbb{Z}$
   (vii) $\forall a, b \in \mathbb{Z}(a \mid b \wedge b \mid a \Rightarrow |a| = |b|)$
   (viii) $\forall a, b \in \mathbb{Z}(a \mid b \Rightarrow \forall c \in \mathbb{Z}(a \mid b \cdot c))$
   (ix) $\forall a, b \in \mathbb{Z}(a \mid b \wedge b \neq 0 \Rightarrow |a| \leq |b|)$
   (x) Dados $a, b, c \in \mathbb{Z}$, c divide a a y a b si y sólo si c divide a cualquier combinación lineal de a y b.
   (xi) $\forall n \in \mathbb{N} \forall a_1, \ldots, a_n, c \in \mathbb{Z}((c|a_1 \wedge \cdots \wedge c|a_n) \Leftrightarrow \forall x_1, x_2, \ldots, x_n \in \mathbb{Z}(c|(x_1 \cdot a_1 + \cdots + x_n \cdot a_n)))$.
   (xii) $\forall a, b, c \in \mathbb{Z}((c \neq 0 \wedge a \cdot c \mid b \cdot c) \Rightarrow a \mid b)$
   (xiii) $\forall a, b, c \in \mathbb{Z}((a \mid b \wedge c \mid d) \Rightarrow a \cdot c \mid b \cdot d)$.

2. Decimos que $z \in \mathbb{Z}$ es par si existe $z' \in \mathbb{Z}$ tal que $z = 2 \cdot z'$, es decir, si 2 divide a z. Decimos que $z \in Z$ es impar si existe $z' \in \mathbb{Z}$ tal que $z = 2 \cdot z' + 1$. Decimos que dos enteros son de la misma paridad si ambos son pares o ambos son impares, en otro caso decimos que son de paridad diferente. Demuestre las siguientes afirmaciones:
   (i) para cualesquiera a, $b \in \mathbb{Z}$, $a + b$ y $a - b$ son de la misma paridad (definición arriba mencionada);
   (ii) $\forall k \in \mathbb{Z}(2 \mid k^2 + k)$;
   (iii) para cualquier $n \in \mathbb{Z}$, si n es impar, entonces $8 \mid (n^2 - 1)$;
   (iv) para cualesquiera a, $b \in \mathbb{Z}$, si a y b son impares, entonces $8 \mid a^2 - b^2$;
   (v) $\forall n \in \mathbb{Z}(4 \nmid (n^2 + 2))$;
   (vi) $\forall n \in \mathbb{Z}(2 \mid (n^2 - n))$;
   (vii) $\forall n \in \mathbb{Z}(6 \mid (n^3 - n))$;
   (viii) para cualesquiera a, $b \in \mathbb{Z}$, si a y b son impares, entonces $a^2 + b^2$ es par, pero $4 \nmid (a^2 + b^2)$.

3. Demuestre que si $a \in \mathbb{Z}$ con $a \neq 0$, entonces el número de divisores de a es finito (Recuerde que un conjunto A es finito si y sólo si existe $n \in \mathbb{N}$ tal que existe $f : I_n \to A$ biyectiva, donde $I_0 = \varnothing$ y si $n \neq 0$, $I_n = \{0, 1, \ldots, n - 1\}$).

4. Demuestre los siguientes criterios de divisibilidad:
   (i) $z \in \mathbb{Z}$ es divisible entre 2 si y sólo si su último dígito es divisible entre 2.
   (ii) $z \in \mathbb{Z}$ es divisible entre 3 si y sólo si la suma de sus dígitos es divisible entre 3.
   (iii) $z \in \mathbb{Z}$ es divisible entre 8 si y sólo si el entero formado por sus 3 últimos dígitos es divisible entre 8.

5. Demuestre que si $u \in \mathbb{Z}$ divide a todos los enteros, entonces u es una unidad en $\mathbb{Z}$.

6. Diga si los siguientes números se pueden escribir como combinación lineal de los números mencionados (*Sugerencia:* utilice el ejercicio (xi) del ejercicio 1)
   (i) 52 como combinación lineal de 20 y 15.
   (ii) 8 como combinación lineal de 18 y 30.
   (iii) 12 como combinación lineal de 30 y 24.

7. Encuentre un número que no sea combinación lineal de 30 y 70.

8. Demuestre que si c es un entero impar, entonces c no es combinación lineal de 98 y 102.

9. Demuestre que si $c = 3n + 1$ o $c = 3n - 1$ para cualquier $n \in \mathbb{Z}$, entonces c no es combinación lineal de 45 y 1251.

10. Demuestre que si d es combinación lineal de a y b, y b es combinación lineal de a y c, entonces d es combinación lineal de a y c.

11. Demuestre el algoritmo de la división, cuidando que cada paso esté bien justificado.

12. Encuentra el cociente y el residuo que se obtiene de dividir a entre b.
    (i) $a = 3111$, $b = 212$
    (ii) $a = 121$, $b = -36$
    (iii) $a = -6411037$, $b = 2164$
    (iv) $a = -24756$, $b = -6108$

13. Demuestre las siguientes afirmaciones, en los casos en que el máximo común divisor esté definido:
    (i) $\forall n, m \in \mathbb{Z}((n; m) = 0 \Leftrightarrow (n = 0 \wedge m = 0))$;
    (ii) $\forall n, m \in \mathbb{Z} \exists \alpha, \beta \in \mathbb{Z}((n; m) = \alpha n + \beta m)$, es decir, el m.c.d. de dos números se puede escribir como combinación lineal de ellos;
    (iii) $\forall k \in \mathbb{Z}((k \mid n \wedge k \mid m) \Rightarrow k \mid (n; m))$;
    (iv) $\forall n, m \in \mathbb{Z}((n; m) = (-n; m) = (n; -m) = (-n; -m))$;

(v) $\forall a, b, c \in \mathbb{Z}((a;(b;c)) = ((a;b);c) = ((a;c);b)$;

(vi) $\forall n, m \in \mathbb{Z}\forall \alpha, \beta \in \mathbb{Z}((n;m) \mid n \cdot \alpha + m \cdot \beta)$;

(vii) $\forall a, b, c \in \mathbb{Z}(a \neq 0 \Rightarrow (a \cdot b; a \cdot c) = |a|(b;c))$.

14. Demuestre las siguientes afirmaciones:

 (i) para cualesquiera $n, m \in \mathbb{Z}$, n y m son primos relativos si y sólo si 1 se puede escribir como combinación lineal de n y m;

 (ii) $\forall a, b, c \in \mathbb{Z}((a \mid b \cdot c \wedge (a;b) = 1) \Rightarrow a \mid c)$;

 (iii) $\forall a, b, c \in \mathbb{Z}((a \mid c \wedge b \mid c \wedge (a;b) = 1) \Rightarrow a \cdot b \mid c)$.

15. Demuestre lo siguiente:

 (i) $\forall a, b \in \mathbb{Z}(a = bq + r \Rightarrow (a;b) = (b;r))$;

 (ii) *Algoritmo de Euclides:* Dados $a, b > 0$, por el Algoritmo de la División, sabemos que hay $q_1, r_1 \in \mathbb{Z}$ tales que $a = b \cdot q_1 + r_1$ y $0 \leq r_1 < b$. Si $r_1 > 0$, por el Algoritmo de la División, sabesmo que hay $q_2, r_2 \in \mathbb{Z}$ tales que $b = r_1 \cdot q_2 + r_2$ y $0 \leq r_2 < r_1$. Si $r_2 > 0$, por el Algoritmo de la División, sabesmo que hay $q_3, r_3 \in \mathbb{Z}$ tales que $r_1 = r_2 \cdot q_3 + r_2$ y $0 \leq r_3 < r_2$. Si continuamos así hasta donde sea posible, obtendremos una sucesión de residuos tales que $b > r_1 \geq r_2 \geq r_3 \geq ... \geq 0$. Demuestre que $(a;b)$ es el último residuo distinto de cero de esta sucesión.

16. Calcule el m.c.d. de las siguientes parejas de números utilizando el Algoritmo de Euclides:

(i) $(6188, 4709)$	(vi) $(78696, 19332)$
(ii) $(1901, 601)$	(vii) $(-2210, 493)$
(iii) $(2184, 1764)$	
(iv) $(34121, 452)$	(viii) $(543, -241)$
(v) $(121, -33)$	(ix) $(-1337, -501)$

17. Demuestre las siguientes afirmaciones:

 (i) 1 tiene exactamente 2 divisores y por ende $1 \notin \mathcal{P}$;

 (ii) 0 tiene más de 4 divisores y por ende $0 \notin \mathcal{P}$;

 (iii) si $p \in \mathcal{P}$, entonces sus cuatro divisores son 1, -1, p y $-p$;

 (iv) 2 y 3 son números primos;

 (v) $\forall p \in \mathcal{P}\forall z \in \mathbb{Z}((p\,;z) = 1 \vee (p\,;z) = |p|)$;

 (vi) $\forall p \in \mathcal{P}\forall z \in \mathbb{Z}(p \nmid z \Rightarrow (p\,;z) = 1)$;

 (vii) $\forall p \in \mathcal{P}\forall a, b \in \mathbb{Z}(p \mid a \cdot b \Rightarrow (p \mid a \vee p \mid b))$;

 (viii) $\forall p \in \mathcal{P}\forall a, b \in \mathbb{Z}((p = a \cdot b \wedge a > 0) \Rightarrow (a = 1 \vee a = |p|))$.

18. Demuestre lo siguiente:

 (i) cualesquiera dos enteros consecutivos son primos relativos;

 (ii) $\forall a, b \in \mathbb{Z}((a;b) = 1 \Rightarrow \forall n, m \in \mathbb{N}(a^n; b^m) = 1)$;

 (iii) $\forall n \in \mathbb{N}^+ \forall a_1, \ldots, a_n, c \in \mathbb{Z}$
 $((\forall i \in \{1, \ldots, n\}(a_i;c) = 1) \Rightarrow (a_1 a_2 \cdots a_n; c) = 1)$.

19. Demuestre lo siguiente sin usar el Teorema Fundamental de la Aritmética:

 (i) Sean $a, p \in \mathbb{Z}$ con $p \neq 1$ tal que p es el mínimo divisor positivo de a, entonces $p \in \mathcal{P}$.

 (ii) Todo entero mayor que 1 es divisible entre un primo. *Sugerencia:* Use el Principio del Buen Orden o el Segundo Principio de inducción.

20. Demuestre las siguientes afirmaciones:

 (i) *Teorema Fundamental de la Aritmética:* si $a \in \mathbb{Z}^+ \setminus \{1\}$, entonces existe un único $k \in \mathbb{N}^+$ y existen únicos $p_1, p_2, ..., p_k \in \mathcal{P}$ tales que $a = p_1 \cdot p_2 \cdot ... \cdot p_k$;

 (ii) si $a \in \mathbb{Z} \setminus \mathbb{Z}^+ \cup \{0, -1\}$, entonces existe un único $k \in \mathbb{N}^+$ y existen únicos $p_1, p_2, ..., p_k \in \mathcal{P}$ tales que $-a = p_1 \cdot p_2 \cdot ... \cdot p_k$;

 (iii) si $a, b, c \in \mathbb{Z}$ y son tales que $a \mid b + c$ y $a \mid b$, entonces $a \mid c$;

 (iv) hay un número infinito de primos, es decir, la cardinalidad de $\mathcal{P}$ es infinita.

21. (a) Encuentre la factorización en primos de los siguientes enteros positivos:

(i) 100	(iv) 109	(vii) 943
(ii) 130	(v) 713	
(iii) 1960	(vi) 503	(viii) 1511

 (b) Diga cuáles son los conjuntos de divisores positivos de cada número del inciso anterior y diga cuántos son.

 (c) Use el inciso (a) para encontrar el máximo común divisor y el mínimo común múltiplo de

 (i) $\{20, -15, 22, -10\}$

 (ii) $\{27, -18, 21, 45\}$

 (iii) $\{168, 842, 252\}$

22. Sea $m \in \mathbb{Z}^+ \setminus \{1\}$ y sea $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_n^{\alpha_n}$ su factorización en primos, donde
$\forall i \in \{1, ..., n\},\ \alpha_i \geq 1$ y $\forall i, j(p_i \neq p_j)$. Demuestre lo siguiente:

 (i) todo divisor positivo de m es de la forma $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_n^{\beta_n}$, con $\forall i \in \{1, ..., n\},\ \beta_i \geq 0$;

 (ii) el número de divisores positivos de m es $(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot ... \cdot (\alpha_n + 1)$.

23. (i) Encuentre un número $z \in \mathbb{Z}$ de forma que tenga exactamente 14 divisores positivos.

 (ii) Encuentre un número $z \in \mathbb{Z}$ de forma que tenga exactamente 12 divisores positivos.

 (iii) Encuentre el menor $z \in \mathbb{Z}^+$ tal que tenga exactamente 14 divisores positivos.

(iv) Encuentre el menor $z \in \mathbb{Z}^+$ tal que tenga exactamente 12 divisores positivos.

24. Demuestre las siguientes afirmaciones, cuando el m.c.d. esté definido:

    (i) $\forall k \in \mathbb{Z}((n \mid k \wedge m \mid k) \implies [n;m] \mid k)$;

    (ii) $\forall n, m \in \mathbb{Z}([n;m] = 0 \iff (n = 0 \vee m = 0))$;

    (iii) $\forall a, b, c \in \mathbb{Z}([a \cdot b; a \cdot c] = |a|[b;c])$;

    (iv) $\forall a, b \in \mathbb{Z}((a;b) = 1 \implies [a;b] = |a \cdot b|)$.

    (v) $\forall a, b \in \mathbb{Z}((a;b)[a;b] = |a \cdot b|)$.

25. Sean $a, b \in \mathbb{Z}^+ \setminus \{1\}$ cuya factorización en primos es $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ y $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}$ con $\forall i \in \{1, ..., n\},\ \alpha_i, \beta_i \geq 0$ (es decir, que algunos de los exponentes pueden ser 0). Demuestre lo siguiente:

    (i) $(a;b) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_n^{\gamma_n}$, donde $\forall i \in \{1, ..., n\},\ \gamma_i = \min\{\alpha_i, \beta_i\}$;

    (ii) $[a;b] = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \ldots \cdot p_n^{\delta_n}$, donde $\forall i \in \{1, ..., n\},\ \delta_i = \max\{\alpha_i, \beta_i\}$.

26. (i) Encuentre el menor múltiplo positivo de 945 que sea un cuadrado.

    (ii) Encuentre el número de divisores de 2160 y calcule la suma de éstos.

    (iii) Si k es el menor entero distinto de cero tal que $1000 \mid k!$, diga cuánto vale la suma de los dígitos de k.

    (iv) Demuestre que para cualquier $n \in \mathbb{Z}$ con $n > 2$, existe un primo p tal que $n < p < n!$.

27. * Revise todos los resultados demostrados sobre la divisibilidad en $\mathbb{Z}$ y diga cuáles son ciertos para cualquier dominio entero, demostrándolos utilizando únicamente la definición de dominio entero y sus implicaciones.

28. Dé un contraejemplo a las siguientes afirmaciones:

    (i) El máximo común divisor se distribuye sobre el mínimo común múltiplo, es decir, para todo $k > 2$ $([m_1; ...; m_{k-1}]; m_k) = [(m_1; m_k); ...; (m_{k-1}; m_k)]$.

    (ii) Si $l > 2$ y $c_1 \mid n$, ..., $c_l \mid n$, entonces $[c_1; ...; c_l] \mid n$.

    (iii) Para todo $k > 2$, se tiene que $(m_1; ...; m_k)[m_1; ...; m_k] = |m_1 \cdot \ldots \cdot m_k|$.

29. Demuestre las siguientes afirmaciones:

    (i) Para cualesquiera $a, b, c \in \mathbb{Z}$, la ecuación diofantina $ax + by = c$ tiene solución si y sólo si $(a;b) \mid c$.

    (ii) Si $a, b \in \mathbb{Z} \setminus \{0\}$ y $(a;b) = 1$, entonces las soluciones de la ecuación diofantina $ax + by = 0$ son $\{(-bz, az) \in \mathbb{Z} \times \mathbb{Z} : z \in \mathbb{Z}\}$, es decir, las soluciones son de la forma $x = -bz$ y $y = az$ para $z \in \mathbb{Z}$.

    (iii) Si $(a;b) \mid c$, el conjunto de soluciones de la ecuación diofantina $ax + by = c$ es $S = (s,t) + \{(\alpha, \beta) : (\alpha, \beta)$ es solución de $ax + by = 0\}$, donde (s,t) es una solución particular de $ax + by = c$.

    (iv) Si $(a;b) \mid c$, el conjunto de soluciones de la ecuación diofantina $ax + by = c$ es $S = (s,t) + \{(\alpha, \beta) : (\alpha, \beta)$ es solución de $\frac{a}{(a;b)}x + \frac{b}{(a;b)}y = 0\}$, donde (s,t) es una solución particular de $ax + by = c$.

30. Diga si las siguientes ecuaciones diofantinas tienen solución, justificando su respuesta y si sí, dé todas sus soluciones:

    (i) $825x + 2975y = 5$

    (ii) $825x + 2975y = 25$

    (iii) $825x + 2975y = -125$

    (iv) $910x + 3003y = 7$

    (v) $910x + 3003y = 91$

    (vi) $910x + 3003y = -364$

    (vii) $33x + 17y = 13$

    (viii) $35x + 17y = 17$

    (ix) $15x + 21y = 10$

    (x) $213x + 441y = 10002$

31. Resuelva los siguientes ejercicios, justificando sus respuestas:

    (i) Supóngase que en la oficina postal se tienen timbres de 5 pesos y de 7 pesos. Entonces, por ejemplo, se pueden mandar cartas a lugares que cuesten 5 pesos, 7 pesos y 12 pesos (con un timbre de 5 y otro de 7) ¿Cuáles son todos los valores que se pueden formar usando estos timbres para mandar cartas?

    (ii) Resuelva el siguiente acertijo propuesto por el astrónomo indio Mahavira en el siglo IX: un grupo de 23 viajeros llega a un campamento y encuentra 63 montones de sacos, todos con el mismo número de sacos, y un montón adicional con 7 sacos. Si sabemos que los viajeros no podían cargar con más de 50 sacos y pudieron repartírselos por igual y sin abrirlos, ¿cuántos sacos había en cada uno de los montones?

    (iii) * Cinco hombres y un mono naufragan en una isla desierta. Los hombres pasan todo el primer día recogiendo cocos. Por la noche, uno de ellos despierta y, desconfiado, decide separar su parte. Divide los cocos en cinco montones, tome su parte y, como sobra un coco, se lo da al mono. Poco después, un segundo náufrago se despierta y hace lo mismo. Al dividir los cocos en cinco montones, vuelve a sobrar un coco y también se lo da al mono. Uno tras otro, el tercero, cuarto y quinto náufragos hacen lo mismo. Al día siguiente por la mañana, dividen los cocos en cinco montones sin que sobre ninguno. ¿Cuántos se habían recolectado inicialmente?