ÁLGEBRA I / MATEMÁTICA DISCRETA I
PRÁCTICO 5 (corresponde al capítulo 3)

1. Dar todos los números primos positivos menores que 100.

2. a) Calcular el máximo común divisor y expresarlo como combinación lineal de los número dados:

   i) 14 y 35 *ii)* 11 y 15 *iii)* 12 y 52 *iv)* 12 y -52 *v)* 12 y 532.

   b) Calcular el mínimo común múltiplo de los números dados en el item (a).

3. Encontrar $(7469, 2464)$, $(2689, 4001)$, $(2447, -3997)$, $(-1109, -4999)$.

4. Dado un entero a, hallar $(0, a)$.

   Respuesta: Todo número entero divide a 0, por lo tanto las únicas condiciones que $d = (0, a)$ debe cumplir es que $d \mid a$ y si $c \mid a$ luego $c \mid d$. Pero $a \mid a$ y por lo tanto $a \mid d$. Tenemos entonces que $d \mid a$ y $a \mid d$ y por lo tanto $d = a$.

5. Probar que si $(a, b) = 1$ y $n+2$ es un número primo, entonces $(a+b, a^2+b^2-nab) = 1$ ó $n+2$.

   Respuesta: Sean a, b y n números enteros tales que $(a, b) = 1$ y $n+2$ es primo, queremos probar que $d := (a+b, a^2+b^2-abn)$ es 1 o $n+2$. Pero $a^2+b^2-abn = (a+b)^2 - ab(n+2)$ y por lo tanto como existen p y q enteros tales que $a+b = p \cdot d$ y $a^2+b^2-abn = (a+b)^2 - ab(n+2) = q \cdot d$ debe existir l entero tal que: $a \cdot b \cdot (n+2) = l \cdot d$. Como $n+2$ es primo tenemos entonces dos posibilidades: **a)** $(n+2) \mid l$ (y por lo tanto existe s entero tal que $l = s \cdot (n+2)$) o **b)** $(n+2) \mid d$ (y por lo tanto existe s entero tal que $d = s \cdot (n+2)$) o

   Si el caso es **a)** entonces $a \cdot b = s \cdot d$ y como $(a+b) = p \cdot d$ tenemos que $d = 1$, ya que $(a \cdot b, a+b) = 1$ si a y b son co-primos (ver siguiente ejercicio).

   Si el caso es **b)** entonces $a \cdot b = s \cdot l$ $(a+b) = p \cdot (n+2) \cdot s$ y por la misma razón que en el caso anterior concluimos que $s = 1$. Pero entonces $d = n+2$.

6. Probar que $(a+b, [a, b]) = (a, b)$. En particular, si dos números son coprimos, también lo son su suma y su producto.

   Respuesta: Primero probaremos dos resultados necesarios:

   a) $(a, b) = d \iff a = m \cdot d \;\; b = n \cdot d$ y $(m, n) = 1$. Prueba: supongamos primero que $(a, b) = d$, entonces existen enteros tales que $a = m \cdot d \;\; b = n \cdot d$, y supongamos que $(m, n) = z$ luego existen enteros p y q tales que $m = p \cdot z$ y $n = q \cdot z$ por lo que $a = m \cdot d = p \cdot z \cdot d$ y $b = n \cdot d = q \cdot z \cdot d$ y vemos que si $c := z \cdot d$, luego $c \mid a$ y $c \mid b$ pero entonces $c \mid d$ y esto solo puede suceder si $z = 1$. Supongamos ahora que $a = m \cdot d \;\; b = n \cdot d$ y $(m, n) = 1$ queremos ver entonces que $(a, b) = d$. Claramente $d \mid a$ y $d \mid b$ por lo tanto solo tenemos que ver que si $c \mid a$ y $c \mid b$ entonces $c \mid d$. Supongamos entonces que existen enteros p y q tales que $a = p \cdot c$ y $b = q \cdot c$. Pero entonces tenemos

$p \cdot cm \cdot d$ y $q \cdot c = n \cdot d$. Expresando a c en sus factores primos podemos ver que todos ellos deben ser factores primos de d, ya que si no lo son debieran ser factores primos de n y m simultáneamente y eso es imposible ya que estos son co-primos. Pero entonces $c \mid d$.

b) Si $(a,b) = 1$ luego $(a+b, a \cdot b) = 1$. Prueba: Sea $d := (a+b, a \cdot b)$, luego sabemos que $a + b = m \cdot d$ y $a \cdot b = m \cdot d$, por otro lado como a y b son co-primos existen enteros s y t tales que $1 = s \cdot a + t \cdot b$.

Por lo tanto:

$$\begin{aligned} s \cdot a + t \cdot (n \cdot d - a) &= 1 \\ (s-t) \cdot a \cdot b + t \cdot n \cdot d \cdot b &= b \\ (s-t) \cdot m \cdot d + t \cdot n \cdot b \cdot d &= b \\ ((s-t) \cdot m + t \cdot n \cdot b) \cdot d &= b \end{aligned}$$

donde en la segunda línea hemos multiplicado por b ambos miembros. Vemos entonces que $d \mid b$. Una cuenta similar (despejando ahora b en función de a) nos indica que también $d \mid a$ y por lo tanto $d \mid 1$, ya que a y b son co-primos, con lo que concluimos que $d = 1$.

Veamos ahora que $(a+b, [a,b]) = (a,b)$. Llamando $d := (a,b)$ tenemos que $a = m \cdot d$ y $b = n \cdot d$, con $(m,n) = 1$. Pero $a + b = (m+n) \cdot d$ y $[a,b] = \frac{a \cdot b}{(a,b)} = m \cdot n \cdot d$ y $(m+n, m \cdot n) = 1$, por lo tanto $(a+b, [a,b]) = d$.

7. Probar que si $n \in \mathbb{Z}$, entonces $2n+1$ y $\frac{1}{2}n(n+1)$ son coprimos.

   Respuesta: Supongamos que no, es decir $d := (2n+1, \frac{1}{2}n \cdot (n+1)) \neq 1$. Luego existe p primo tal que $p \mid d$. Pero entonces $p \mid (2n+1)$ y $p \mid \frac{1}{2}n \cdot (n+1) \Rightarrow p \mid 2 \cdot \frac{1}{2}n \cdot (n+1) \Rightarrow p \mid n \cdot (n+1)$. Pero entonces tenemos dos casos: **1)** $p \mid n$ o **2)** $p \mid (n+1)$. En el primer caso $p \mid n$ y como $p \mid (2n+1)$ tenemos que $p \mid (2n+1-2 \cdot n)$ o sea $p \mid 1$ y llegamos a una contradicción. En el segundo caso $p \mid (n+1)$ y por lo tanto $p \mid (2n+2)$, pero como $p \mid (2n+1)$, $p \mid (2n+2-(2n+1))$ y nuevamente llegamos a una contradicción ya que concluimos que $p \mid 1$.

8. Probar: **i)** $(a,b) = 1$, $a \mid c$ y $b \mid c$, $\Rightarrow ab \mid c$.

   ii) $(a,b) = 1$ y $a \mid bc \Rightarrow a \mid c$.

   Respuestas:

   i) Si $a \mid c$ y $b \mid c$ entonces $[a,b] \mid c$. Pero como $(a,b) = 1$ tenemos que $[a,b] = a \cdot b$ y por lo tanto $a \cdot b \mid c$.

   ii) Si $a \mid bc$ y como $b \mid b \cdot c$ entonces por **i)** $a \cdot b \mid bc$ y por lo tanto $a \mid c$.

9. a) Probar que el producto de tres enteros consecutivos es divisible por 6.

   b) Probar que el producto de cuatro enteros consecutivos es divisible por 24.

   Respuesta:

   a) Si n es el primero de los tres números el producto es: $n(n+1)(n+2)$. Dado cualquier n este se puede escribir como $n = 3k + r$ con $k, r \in \mathbb{Z}$, $0 \leq r < 3$. En el caso $r = 0$ tenemos que el producto es: $3k(3k+1)(3k+2)$ y es cláramente divisible por 3. En el segundo caso, $r = 1$ tenemos que el producto es: $(3k+1)(3k+2)(3K+3) = (3k+1)(3k+2)3(K+1)$ que es divisible por 3. Para el caso $r = 2$ tenemos $(3k+2)(3K+3)(3k+4) = (3k+2)3(K+1)(3k+4)$ que también es divisible por 3.

10. Demostrar que $\forall n \in \mathbb{Z}$, $n > 2$, existe p primo tal que $n < p < n!$. (Ayuda: pensar qué primos dividen a $n! - 1$.)

    Respuesta: Consideremos el número $n! - 1$ como es mayor que 1 lo podemos desarrollar en sus factores primos obteniendo:

    $$n! - 1 = \prod_{i=1}^{m} p_i$$

    Claramente $p_i \leq n! - 1$. Tomemos uno cualquiera de estos factores primos, q. Como este divide a $n! - 1$ tenemos que $n! = b \cdot q + 1$ para algún entero b. Pero entonces $q > n$ ya que de otra manera dividiria a $n!$.

11. Completar y demostrar:

    Respuestas:

    a) Si $a \in \mathbb{Z}$, entonces $[a, a] = a$.

    Claramente $(a, a) = a$ y por lo tanto $[a, a] = \frac{a^2}{(a,a)} = a$.

    b) Si a, $b \in \mathbb{Z}$, $[a, b] = b$ si y sólo si $a \mid b$.

    Si $a \mid b$ entonces $(a, b) = a$ y por lo tanto $[a, b] = \frac{a \cdot b}{(a,b)} = b$.

    c) $(a, b) = [a, b]$ si y sólo si $|a| = |b|$.

    Supongamos $a > 0$, $b > 0$, luego $(a, b) \leq \min\{a, b\}$ y $[a, b] \geq \max\{a, b\}$. Pero entonces $\min\{a, b\} = \max\{a, b\}$ y por lo tanto $a = b$.

12. ¿Existen enteros m y n tales que:

    a) $m^4 = 27$? **b)** $m^2 = 12n^2$? **c)** $m^3 = 47n^3$?

    Respuestas: **a)** Imposible ya que $27 = 3^3$ mientras que la decomposición en factores primos de m^4 solo tiene primos elevados a potencias múltiplos de 4.

13. Encontrar todos los enteros positivos a y b tales que $(a, b) = 10$, y $[a, b] = 100$.

14. Si ab es un cuadrado y a y b son coprimos, probar que a y b son cuadrados.

    Respuesta: Como a y b son co-primos entonces sus decomposiciones en factores primos no tienen ningún factor en común. Como su producto es un cuadrado entonces estos primos tienen que tener potencias pares, con lo que vemos que cada uno debe ser un cuadrado.

15. Mostrar que 725 y 441 son coprimos y encontrar enteros m, n tales que $1 = m.725+n.441$.

16. Probar que $\sqrt{6}$ es irracional.

17. Probar que $2^{3n+1} + 7^{3n+1}$ es divisible por 9 para todo $N \in \mathbb{N}$, n par.

    Respuesta: $2^{3n+1} + 7^{3n+1} = 2^{3n+1} + (9-2)^{3n+1} = 2^{3n+1} + \sum_{i=0}^{3n+1} \binom{i}{2n+1-i} 9^i (-2)^{3n+1-i}$ El primer término es $(-2)^{3n+1} = -2^{3n+1}$ ya que se n es par. Este término se cancela con el primer término y entonces nos queda una sumatoria donde cada uno de sus términos tiene al menos un 9 multiplicando. Por lo tanto es divisible por 9.

18. Calcular el máximo común divisor entre 606 y 108 y expresarlo como combinación lineal de esos números.

19. Probar que todo entero impar que no es múltiplo de 3 es de la forma $6m \pm 1$ para algún $m \in \mathbb{Z}$.

    Respuesta: Si no es divisible por 3 entonces es de la forma $p = 3k+1$ o $3k+2$ para alún k entero. En el primer caso, si además debe ser par entonces $k = 2n$ y por lo tanto $p = 3k+1 = 3 \cdot 2n + 1 = 6m+1$. En el segundo caso k debe ser impar y por lo tanto de la forma $k = 2n+1$ con lo que obtenemos $p = 3k+2 = 3(2n+1)+2 = 6n+6-1 = 6(n+1)-1$.

20. Probar que si d es un divisor común de a y b, entonces

    $$a)\ \frac{(a,b)}{d} = (\frac{a}{d}, \frac{b}{d}). \qquad b)\ \frac{[a,b]}{d} = [\frac{a}{d}, \frac{b}{d}].$$

    Respuesta: Si $d \mid a$ y $d \mid b$ entonces $a = m \cdot d$ y $b = n \cdot d$. Sea $(m,n) = l$, entonces $m = p \cdot l$ y $n = q \cdot l$ con $p, q) = 1$. Por lo tanto $a = p \cdot l \cdot d$ y $b = q \cdot l \cdot d$ lo que implica $(a,b) = l \cdot d$ (ya que $p, q) = 1$). Y tenemos así que $\frac{(a,b)}{d} = l = (m,n)$.

21. Probar que para todo $n \in \mathbb{Z}$, $n^2 + 2$ no es divisible por 4.

    Respuesta: Ver por separado el caso en que n es par o impar y usar el teorema del resto.

22. Dado un entero $a > 0$ fijo, caracterizar aquellos números que al dividirlos por a tienen cociente igual al resto.

    Respuesta: Queremos los números n tales que $n = r \cdot q + r$ Pero $n = r \cdot q + r = r(q+1)$ o sea son todos los números que son divisibles por $q+1$.

23. Sea p primo positivo. Probar que $(p, (p-1)!) = 1$.

    Respuesta: $(p-1)! = \prod_{i=1}^{m} q_i^{h_i}$ con $q_i \leq p-1 < p$ ya que este producto es a su vez el producto de los factores primos de cada uno de los números de la productoria del factorial y cada uno de estos es menor que $p-1$. Pero entonces p y $(p-1)!$ son co-primos.

24. Hallar el menor múltiplo de 168 que sea un cuadrado.

    Respuesta: $168 = 2^3 \cdot 3 \cdot 7$ por lo tanto el menor múltiplo de 168 que es un cuadrado es $2^2 \cdot 3^2 \cdot 7^2 = 42 \cdot 168$.

25. Probar que si $(a,4) = 2$ y $(b,4) = 2$ entonces $(a+b, 4) = 4$.

    Respuesta: $(a,4) = 2 \;\Rightarrow a = 2m\ 4 = 2p$ con $(m,p) = 1$. Pero $p = 2$ y por lo tanto $(m,2) = 1$ con lo que concluimos que m es impar. Haciendo lo mismo con b obtenemos $b = 2n$ con n impar. Pero luego $n+m$ es par, con lo que sigue que $a+b = 2m+2n = 2(m+n) = 4l$ para algún entero l. Tenemos asi, $(a+b, 4) = (4l, 4) = 4$.

26. Probar que el producto de dos enteros consecutivos no nulos no es un cuadrado. (Ayuda: usar el Teorema Fundamental de la Aritmética).

    Respuesta: El caso $n = 1$ es trivial. Es facil ver que $(n, n+1) = 1$ por lo tanto no tienen ningún factor primo en común. Esto implica que cada uno de ellos debe ser a su vez un cuadrado. Pero es facil ver que si n es un cuadrado su consecutivo no lo puede ser (ya que $(k+1)^2 - (k^2+1) = 2k$)