Práctico 3
Matemática Discreta I – Año 2020/1
FAMAF

Ejercicios resueltos

1. Hallar el cociente y el resto de la división de:
   a) 135 por 23, *Rta:* Como $135 = 23 \cdot 5 + 20$ entonces $q = 5, r = 20$, ya que $0 \leq 20 < 23 = |23|$.
   b) -135 por 23, *Rta:* Por el item anterior $-135 = -23 \cdot 5 - 20$, pero $-20 < 0$; hay que corregirlo, y se hace restando y sumando el módulo del divisor:
   $$-135 = (-23 \cdot 5 - 23) + (23 - 20) = 23 \cdot (-6) + 3.$$
   De donde $q = -6, r = 3$.
   c) 135 por -23, *Rta:* $135 = (-23) \cdot (-5) + 20$; luego $q = -5, r = 20$, ya que $0 \leq 20 < 23 = |-23|$.
   d) -135 por -23, *Rta:* $-135 = 23 \cdot (-6) + 3 = (-23) \cdot 6 + 3$, entonces $q = 6, r = 3$ $(0 \leq 3 < 23 = |-23|)$.
   e) 127 por 99, *Rta:* $127 = 99 \cdot 1 + 28$; $q = 1, r = 28$.
   f) 98 por 73. *Rta:* $98 = 73 \cdot 1 + 25$; $q = 1, r = 25$.

2. *a*) Si $a = b \cdot q + r$, con $b \leq r < 2b$, hallar el cociente y el resto de la división de a por b.
   Rta: $a = b \cdot (q + 1) + (r - b)$, con $0 \leq r - b < b$, por lo tanto el cociente es $q + 1$ y el resto $r - b$.
   b) Repetir el ejercicio anterior, suponiendo ahora que $-b \leq r < 0$.
   Rta: $a = b \cdot (q - 1) + (r + b)$, con $0 \leq r + b < b$, por lo tanto el cociente es $q - 1$ y el resto $r + b$.

3. Dado $m \in \mathbb{N}$ hallar los restos posibles de m^2 y m^3 en la division por $3, 4, 5, 7, 8, 11$.
   Rta: El resto del cuadrado (cubo) de m es el resto del cuadrado (cubo) del resto de m. Por lo tanto hay que calcular los restos $\tilde{r}$ de r^2 con $0 \leq r < m$. Así tenemos para $m = 3, \tilde{r} \in \{0, 1\}$; $m = 4, \tilde{r} \in \{0, 1\}$; $m = 5, \tilde{r} \in \{0, 1, 4\}$; $m = 7, \tilde{r} \in \{0, 1, 2, 4\}$; $m = 8, \tilde{r} \in \{0, 1, 4\}$; $m = 11, \tilde{r} \in \{0, 1, 3, 4, 5, 9\}$.

4. Expresar en base 10 los siguientes enteros:
   a) $(1503)_6$ *Rta:* $1 \cdot 6^3 + 5 \cdot 6^2 + 0 \cdot 6^1 + 3 \cdot 6^0 = 216 + 5 \cdot 36 + 3 = 399$.

b) $(1111)_2$ *Rta:* $2^3 + 2^2 + 2^1 + 2^0 = 8 + 4 + 2 + 1 = 15$

c) $(1111)_{12}$ *Rta:* $12^3 + 12^2 + 12^1 + 1 = \dfrac{12^4 - 1}{11} = \dfrac{144^2 - 1}{11} = \dfrac{143 \cdot 145}{11} = 13 \cdot 145 = 1885$.

d) $(123)_4$ *Rta:* $1 \cdot 4^2 + 2 \cdot 4 + 3 = 27$.

e) $(12121)_3$ *Rta:* $3^4 + 2 \cdot 3^3 + 3^2 + 2 \cdot 3^1 + 3 = 81 + 54 + 9 + 6 + 3 = 153$.

f) $(1111)_5$ *Rta:* $5^3 + 5^2 + 5^1 + 1 = \dfrac{5^4 - 1}{4} = \dfrac{624}{4} = 156$.

5. Convertir

a) $(133)_4$ a base 8,

Rta: Debemos primero calcular cuanto vale $(133)_4$ en base 10 (la base usual) y luego pasarlo a base 8. Ahora bien, $(133)_4 = 4^2 + 3 \cdot 4 + 3 = 31$, y $31 = 3 \cdot 8 + 7$, por lo tanto $(133)_4 = (37)_8$.

b) $(B38)_{16}$ a base 8,

Rta: Aquí usaremos que $16 = 2 \cdot 8$. Entonces, $(B38)_{16} = 11 \cdot 16^2 + 3 \cdot 16 + 8 = 44 \cdot 8^2 + 6 \cdot 8 + 8 = (5 \cdot 8 + 4) \cdot 8^2 + 7 \cdot 8 = 5 \cdot 8^3 + 4 \cdot 8^2 + 7 \cdot 8 = (5470)_8$.

c) $(3506)_7$ a base 2,

Rta: $(3506)_7 = 3 \cdot 7^3 + 5 \cdot 7^2 + 6 = 1280$. Ahora debemos escribir 1280 en base 2:

$$\begin{aligned}
1280 &= 2 \cdot 640 + 0\\
640 &= 2 \cdot 320 + 0\\
320 &= 2 \cdot 160 + 0\\
160 &= 2 \cdot 80 + 0\\
80 &= 2 \cdot 40 + 0\\
40 &= 2 \cdot 20 + 0\\
20 &= 2 \cdot 10 + 0\\
10 &= 2 \cdot 5 + 0\\
5 &= 2 \cdot 2 + 1\\
2 &= 2 \cdot 1 + 0\\
1 &= 2 \cdot 0 + 1.
\end{aligned}$$

Luego $(3506)_7 = (10100000000)_2$.

Hay una forma de hacer este ejercicio más corta: observar que $1280 = 2^7 \cdot 10 = 2^8 \cdot 5 = 2^8 \cdot (2^2 + 1) = 2^{10} + 2^8$.

d) $(1541)_6$ a base 4.
Rta: $6^3 + 5 \cdot 6^2 + 4 \cdot 6 + 1 = 54 \cdot 4 + 45 \cdot 4 + 6 \cdot 4 = 105 \cdot 4 = 420$. Luego,

$$\begin{aligned} 420 &= 4 \cdot 105 + 0 \\ 105 &= 4 \cdot 26 + 1 \\ 26 &= 4 \cdot 6 + 2 \\ 6 &= 4 \cdot 1 + 2 \\ 1 &= 4 \cdot 0 + 1. \end{aligned}$$

Entonces, $(1541)_6 = (12210)_4$.

6. Calcular:

a) $(2234)_5 + (2310)_5$
Rta: La suma entre números escritos en la misma base se hace de la misma forma que la suma usual, teniendo en cuenta que en base 5 tenemos $2 + 3 = (10)_5$, $3 + 3 = (11)_5$, etc.

$$\begin{array}{r} (2234)_5 \\ +(2310)_5 \\ \hline (10044)_5 \end{array}$$

b) $(10101101)_2 + (10011)_2$ *Rta:* $(11000000)_2$.

7. Sean a, b, $c \in \mathbb{Z}$. Demostrar las siguientes afirmaciones:

a) Si $ab = 1$, entonces $a = b = 1$ ó $a = b = -1$.
Rta: Notar que a y b no pueden ser nulos, y si tienen distinto signo su producto es negativo, luego podemos suponer que son ambos positivos o negativos. Si $a > 1$ entonces $1 = ab > b > 0$, lo cual es absurdo. Igualmente si $a < -1$ entonces $1 = ab > -b > 0$. Luego $a = \pm 1$ y entonces $b = \pm 1$.

b) Si $a, b \neq 0$, $a|b$ y $b|a$, entonces $a = b$ ó $a = -b$.
Rta: Tenemos que existen $p, q \in \mathbb{Z}$ tales que $b = ap$ y $a = bq$. Luego, $a = apq$ y $a \neq 0 \Rightarrow pq = 1$. El inciso a) dice que $p = q = 1$ ó $p = q = -1$, de donde se sigue el resultado buscado.

c) Si $a|1$, entonces $a = 1$ ó $a = -1$.

Rta: Este es un corolario del inciso *b)* tomando $b = 1$ ya que $1|a$, $\forall a \in \mathbb{Z}$.

d) Si $a \neq 0$, $a|b$ y $a|c$, entonces $a|(b+c)$ y $a|(b-c)$.

Rta: Como existen $p, q \in \mathbb{Z}$ tales que $b = ap$ y $c = aq$, $b \pm c = a(p \pm q)$.

e) Si $a \neq 0$, $a|b$ y $a|(b+c)$, entonces $a|c$.

Rta: Por el inciso anterior: $a|((b+c)-b)$, o lo que es lo mismo $a|c$.

f) Si $a \neq 0$ y $a|b$, entonces $a|b \cdot c$.

Rta: Si $b = aq$, para algún $q \in \mathbb{Z}$, entonces $b \cdot c = aqc \Rightarrow a|b \cdot c$.

8. Dados b, c enteros, probar las siguientes propiedades:

a) 0 es par y 1 es impar.

Rta: $0 = 2 \cdot 0$ y $1 = 2 \cdot 0 + 1$.

b) Si b es par y $b \mid c$, entonces c es par. (Por lo tanto, si b es par, también lo es $-b$).

Rta: Existen $p, q \in \mathbb{Z}$ tales que $b = 2q, c = bp \Rightarrow c = 2qp \Rightarrow c$ es par. $(b|-b)$.

c) Si b y c son pares, entonces $b + c$ también lo es.

Rta: $2|b, 2|c \Rightarrow 2|(b+c)$.

d) Si un número par divide a 2, entonces ese número es 2 ó -2.

Rta: Dicho número a no puede ser 0, y por el ejercicio 7 b): $2|a$ y $a|2 \Longrightarrow a = \pm 2$.

e) La suma de un número par y uno impar es impar.

Rta: Existen $p, q \in \mathbb{Z}$ tales que $a = 2q, b = 2p + 1 \Rightarrow a + b = 2(q+p) + 1$.

f) $b + c$ es par si y sólo si b y c son ambos pares o ambos impares.

Rta: Si b y c son ambos pares, entonces por el ejercicio 7 c): $b+c$ es par; ahora si existen $p, q \in \mathbb{Z}$ tales que $b = 2q+1, c = 2p+1 \Rightarrow b+c = 2q+1+2p+1 = 2(q+p+1)$.

De otro lado, notar que por el inciso anterior la única posibilidad para que $b + c$ sea par es que b y c sean ambos pares ó ambos impares.

9. Sea $n \in \mathbb{Z}$. Probar que n es par si y sólo si n^2 es par.

Rta: $[\Rightarrow]$ Si existe $q \in \mathbb{Z}$ tal que $n = 2q$, entonces $n^2 = 2(2q^2)$.

$[\Leftarrow]$ Demostremos el contrarecíproco. En efecto, si existe $p \in \mathbb{Z}$ tal que $n = 2p + 1$, entonces $n^2 = 4p^2 + 4p + 1 = 2(2p^2 + 2p) + 1$.

10. Probar que $n(n+1)$ es par para todo n entero.

Rta: Si $n = 2q$, para algún $q \in \mathbb{Z}$, $n(n+1) = 2q(2q+1)$ es par. Si $n = 2p+1$, para algún $p \in \mathbb{Z}$, $n(n+1) = (2p+1)(2p+1+1) = 2(p+1)(2p+1)$ es par.

11. Sean a, b, $c \in \mathbb{Z}$. ¿Cuáles de las siguientes afirmaciones son verdaderas? Justificar las respuestas.

   a) $a \mid b \cdot c \Rightarrow a \mid b$ ó $a \mid c$.

   Rta: Falso, contraejemplo: $6|12 = 4 \cdot 3$ pero 6 no divide a 4 ni divide a 3.

   b) $a \mid (b+c) \Rightarrow a \mid b$ ó $a \mid c$.

   Rta: Falso, contraejemplo: $6|(5+1)$ pero 6 no divide a 5 ni a 1.

   c) $a \mid c$ y $b \mid c \Rightarrow a \cdot b \mid c$.

   Rta: Falso, contraejemplo: $6|12$ y $4|12$ pero 24 no divide a 12.

   d) $a \mid c$ y $b \mid c \Rightarrow (a+b) \mid c$.

   Rta: Falso, contraejemplo: $2|6$ y $3|6$ pero $5 = 2+3$ no divide a 6.

   e) a, b, $c > 0$ y $a = b \cdot c$, entonces $a \geq b$ y $a \geq c$.

   Rta: Verdadero, $b \geq 1 \Rightarrow a = bc \geq c$ y $c \geq 1 \Rightarrow a = bc \geq b$.

12. Probar que cualquiera sea $n \in \mathbb{N}$:

   a) $3^{2n+2} + 2^{6n+1}$ es múltiplo de 11.

   Rta: $3^{2n+2} + 2^{6n+1} = 9^n \cdot 9 + 64^n \cdot 2$. Como el resto de dividir 64 por 11 es 9, tenemos que $9^n \cdot 9 + 64^n \cdot 2$ es divisible por 11 si $9^n \cdot 9 + 9^n \cdot 2$ lo es y este último es $9^n(9+2)$ que claramente es divisible por 11.

   Rta Alternativa: podemos probar por inducción. Si $n = 1$, $3^4 + 2^7 = 209$ y $11 \mid 209$. Supongamos que para algún $k \in \mathbb{N}$, $11 \mid 3^{2k+2} + 2^{6k+1}$ (HI). Debemos probar que

$$11 \mid 3^{2(k+1)+2} + 2^{6(k+1)+1} \Leftrightarrow 11 \mid 3^{2k+4} + 2^{6k+7}.$$

   Ahora bien,

$$\begin{aligned} 3^{2k+4} + 2^{6k+7} &= 3^2 3^{2k+2} + 2^6 2^{6k+1} \\ &= 9 \cdot 3^{2k+2} + 64 \cdot 2^{6k+1} \\ &= 9(3^{2k+2} + 2^{6k+1}) + 55 \cdot 2^{6k+1}. \end{aligned}$$

   Es claro que el primer término es divisible por 11 por HI. El segundo término es $55 \cdot 2^{6k+1}$ que es divisible por 11, pues 55 lo es. Concluyendo $9(3^{2k+2} + 2^{6k+1}) + 55 \cdot 2^{6k+1}$ es divisible por 11 y por lo tanto $11|3^{2k+4} + 2^{6k+7}$.

b) $3^{2n+2} - 8n - 9$ es divisible por 64.

Rta: Lo haremos por inducción. El caso base es $n = 1$ y en ese caso debemos ver que $64 \mid 3^{2\cdot 1+2} - 8 \cdot 1 - 9 = 3^4 - 8 - 9 = 81 - 17 = 64$, lo cual esta bien. Supongamos que para algún $k \in \mathbb{N}$, $64 \mid 3^{2k+2} - 8k - 9$ (HI), entonces debemos probar que $64 \mid 3^{2(k+1)+2} - 8(k+1) - 9 = 9 \cdot 3^{2k+2} - 8k - 17$.

Ahora bien,

$$\begin{aligned} 9 \cdot 3^{2k+2} - 8k - 17 &= 9 \cdot (3^{2k+2} - 8k - 9 + 8k + 9) - 8k - 17 \\ &= 9 \cdot (3^{2k+2} - 8k - 9) + 9 \cdot (8k + 9) - 8k - 17 \\ &= 9 \cdot (3^{2k+2} - 8k - 9) + 72k + 81 - 8k - 17 \\ &= 9 \cdot (3^{2k+2} - 8k - 9) + 64(k + 1). \end{aligned}$$

El primer término es múltiplo de 64 por HI y el segundo es $64(k + 1)$ que claramente es múltiplo de 64.

13. Decir si es verdadero o falso justificando:

a) $3^n + 1$ es múltiplo de n, $\forall n \in \mathbb{N}$.

Rta: Falso, contraejemplo $n = 3$.

b) $3n^2 + 1$ es múltiplo de 2, $\forall n \in \mathbb{N}$.

Rta: Falso, contraejemplo $n = 2$.

c) $(n + 1) \cdot (5n + 2)$ es múltiplo de 2, $\forall n \in \mathbb{N}$.

Rta: Verdadero. Si n es par, $5n + 2$ es par y por lo tanto $(n + 1) \cdot (5n + 2)$ es múltiplo de 2. Si n es impar, $n + 1$ es par y $2 \mid (n + 1) \cdot (5n + 2)$.

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

Rta: Si n es impar, $n^2 + 2$ es impar y por lo tanto no es divisible por 4. Si n es par, n^2 es divisible por 4 y como 4 no divide a 2 entonces 4 no divide a $n^2 + 2$.

15. Probar que todo entero impar que no es múltiplo de 3, es de la forma $6m \pm 1$, con m entero.

Rta: Como n no es divisible por 3, debe ser $n = 3q \pm 1$, para algún $q \in \mathbb{Z}$. Si q fuese impar entonces n sería par, por lo tanto $q = 2m$, con $m \in \mathbb{Z}$, y obtenemos el resultado.

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

Rta: Sea $n \in \mathbb{Z}$. Debemos probar que $6 \mid n(n + 1)(n + 2)$. Si alguno de los tres enteros es cero, entonces el resultado ya se cumple pues $6 \mid 0$. Además, si $a, b, c \in \mathbb{N}$ entonces $(-a)(-b)(-c) = -(abc)$. De todo lo anterior, basta con probar que $6 \mid n(n+1)(n+2)$ para todo $n \in \mathbb{N}$. Esto se puede hacer por inducción, pero usaremos números combinatorios: $\forall n \in \mathbb{N}$,

$$\binom{n+2}{3} = \frac{(n+2)!}{3!(n-1)!} = \frac{n(n+1)(n+2)}{3!}.$$

Por lo tanto, $n(n+1)(n+2) = 6 \cdot \binom{n+2}{3}$, y como $\binom{n+2}{3} \in \mathbb{N}$, se sigue que $6 \mid n(n+1)(n+2)$.

Rta Alternativa: Por el ejercicio 10 sabemos que $2 \mid n(n+1)(n+2)$. Como $(2,3) = 1$, basta probar que $3 \mid n(n+1)(n+2)$. Para esto, consideremos los restos de dividir a n por 3:

- Si $n = 3q$, para algún $q \in \mathbb{Z}$, entonces $n(n+1)(n+2) = 3q(n+1)(n+2)$.
- Si $n = 3p+1$, para algún $p \in \mathbb{Z}$, entonces $n+2 = 3(p+1)$, de donde $n(n+1)(n+2) = 3n(n+1)(p+1)$.
- Si $n = 3r+2$, para algún $r \in \mathbb{Z}$, luego $n+1 = 3(r+1) \Rightarrow n(n+1)(n+2) = 3n(r+1)(n+2)$.

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

Rta: Sea $n \in \mathbb{Z}$. Debemos demostrar que $24 \mid n(n+1)(n+2)(n+3)$. Como $24 \mid 0$, y si $a, b, c, d \in \mathbb{N}$ entonces $(-a)(-b)(-c)(-d) = abcd$, basta con probar que $24 \mid n(n+1)(n+2)(n+3)$ para todo $n \in \mathbb{N}$. Tenemos que $\forall n \in \mathbb{N}$,

$$\binom{n+3}{4} = \frac{(n+3)!}{4!(n-1)!} = \frac{n(n+1)(n+2)(n+3)}{4!}.$$

Por lo tanto, $n(n+1)(n+2)(n+3) = 24 \cdot \binom{n+3}{4} \Rightarrow 24 \mid n(n+1)(n+2)(n+3)$.

Rta Alternativa: Por el inciso *a*) sabemos que $3 \mid n(n+1)(n+2)(n+3)$. Como $(3,8) = 1$, basta probar que $8 \mid n(n+1)(n+2)(n+3)$. Para esto, consideremos si n es par ó impar:

- Si $n = 2q$, para algún $q \in \mathbb{Z}$, entonces

$$\begin{aligned} n(n+1)(n+2)(n+3) &= 2q(n+1)(2q+2)(n+3) \\ &= 4q(q+1)(n+1)(n+3). \end{aligned}$$

  Pero, $q(q+1) = 2r$, para algún $r \in \mathbb{Z}$, de donde $n(n+1)(n+2)(n+3) = 8r(n+1)(n+3)$.

- Si $n = 2p+1$, para algún $p \in \mathbb{Z}$, entonces $n(n+1)(n+2)(n+3) = n(2p+2)(n+2)(2p+4) = 4n(p+1)(p+2)(n+2)$. Pero, $(p+1)(p+2) = 2s$, para algún $s \in \mathbb{Z}$, luego $n(n+1)(n+2)(n+3) = 8sn(n+2)$.

17. Probar que si a y b son enteros entonces a^2+b^2 es divisible por 7 si y sólo si a y b son divisibles por 7. ¿Es lo mismo cierto para 3? ¿Para 5?
Rta: Los restos posibles de dividir por 7 son 0,1,2,3,4,5,6. Los restos de sus cuadrados son $0,1,2,4$. La única suma de dos de ellos que da un múltiplo de 7 es $0+0=0$. Luego a^2+b^2 sólo puede ser divisible por 7 si a y b lo son. En el caso de 3, tenemos que los restos de cuadrados posibles son 0 y 1, y para que la suma de 0 solo puede ser $0+0$, como en el caso anterior. Para el caso del 5, tenemos 1^2+2^2 es divisible por 5 pero 1 y 2 no lo son.

18. Encontrar $(7469, 2464)$, $(2689, 4001)$, $(2447, -3997)$, $(-1109, -4999)$.
Rta 1: $7469 = 3 \cdot 2464 + 77$, $2464 = 32 \cdot 77$. Por lo tanto, $(2469, 2464) = 77$.
Rta 2: $4001 = 2689 + 1312$, $2689 = 2 \cdot 1312 + 65$, $1312 = 20 \cdot 65 + 12$, $65 = 5 \cdot 12 + 5$, $12 = 2 \cdot 5 + 2$, $5 = 2 \cdot 2 + 1$. Por lo tanto, $(2689, 4001) = 1$.
Rta 3: $-3997 = (-2)2447 + 897$, $2447 = 2 \cdot 897 + 653$, $897 = 653 + 244$, $653 = 2 \cdot 244 + 165$, $244 = 165 + 79$, $165 = 2 \cdot 79 + 7$, $79 = 11 \cdot 7 + 2$, $7 = 3 \cdot 2 + 1$. Por lo tanto, $(2447, -3997) = 1$.
Rta 4: $4999 = 4 \cdot 1109 + 563, 1109 = 563 + 546, 563 = 546 + 17, 546 = 17 \cdot 32 + 2,$ $17 = 2 \cdot 8 + 1$. Por lo tanto, $(-1109, -4999) = (1109, 4999) = 1$.

19. Calcular el máximo común divisor y expresarlo como combinación lineal de los números dados, para cada uno de los siguientes pares de números:
    a) 14 y 35, *Rta:* $35 = 2 \cdot 14 + 7; 14 = 2 \cdot 7; (14, 35) = 7 = -2 \cdot 14 + 35$.
    b) 11 y 15, *Rta:* $15 = 11 + 4; 11 = 2 \cdot 4 + 3; 4 = 3 + 1;$
    $$1 = 4 - 3 = 15 - 11 - (11 - 2 \cdot (15 - 11)) = 3 \cdot 15 - 4 \cdot 11.$$
    c) 12 y 52, *Rta:* $(12, 52) = 4 = 52 - 4 \cdot 12$.
    d) 12 y -52, *Rta:* $(12, -52) = 4 = -4 \cdot 12 - (-52)$.
    e) 12 y 532, *Rta:* $(12, 532) = 4 = -44 \cdot 12 + 532$.
    f) 725 y 441,

Rta:

$$
\begin{array}{rcr}
725 = 441 \cdot 1 + 284 & \Rightarrow & 284 = 725 - 441 \\
441 = 284 \cdot 1 + 157 & \Rightarrow & 157 = 441 - 284 \\
284 = 157 \cdot 1 + 127 & \Rightarrow & 127 = 284 - 157 \\
157 = 127 \cdot 1 + 30 & \Rightarrow & 30 = 157 - 127 \\
127 = 30 \cdot 4 + 7 & \Rightarrow & 7 = 127 - 30 \cdot 4 \\
30 = 7 \cdot 4 + 2 & \Rightarrow & 2 = 30 - 7 \cdot 4 \\
7 = 2 \cdot 3 + 1 & \Rightarrow & 1 = 7 - 2 \cdot 3 \\
2 = 1 \cdot 2 + 0. & &
\end{array}
$$

Luego $(725, 441) = 1$ y

$$
\begin{aligned}
1 &= 7 - 2 \cdot 3 \\
&= 7 - (30 - 7 \cdot 4) \cdot 3 = 7 \cdot 13 - 30 \cdot 3 \\
&= (127 - 30 \cdot 4) \cdot 13 - 30 \cdot 3 = 127 \cdot 13 - 55 \cdot 30 \\
&= 127 \cdot 13 - 55 \cdot (157 - 127) = 68 \cdot 127 - 55 \cdot 157 \\
&= 68 \cdot (284 - 157) - 55 \cdot 157 = 68 \cdot 284 - 123 \cdot 157 \\
&= 68 \cdot 284 - 123 \cdot (441 - 284) = 191 \cdot 284 - 123 \cdot 441 \\
&= 191 \cdot (725 - 441) - 123 \cdot 441 = 191 \cdot 725 - 314 \cdot 441.
\end{aligned}
$$

Es decir, $1 = 191 \cdot 725 - 314 \cdot 441$.

g) 606 y 108.

Rta:

$$
\begin{array}{rcr}
606 = 108 \cdot 5 + 66 & \Rightarrow & 66 = 606 - 108 \cdot 5 \\
108 = 66 \cdot 1 + 42 & \Rightarrow & 42 = 108 - 66 \\
66 = 42 \cdot 1 + 24 & \Rightarrow & 24 = 66 - 42 \\
42 = 24 \cdot 1 + 18 & \Rightarrow & 18 = 42 - 24 \\
24 = 18 \cdot 1 + 6 & \Rightarrow & 6 = 24 - 18 \\
18 = 6 \cdot 3 + 0 & &
\end{array}
$$

Luego $(606, 108) = 6$ y

$$\begin{aligned} 6 &= 24 - 18 \\ &= 24 - (42 - 24) = 2 \cdot 24 - 42 \\ &= 2 \cdot (66 - 42) - 42 = 2 \cdot 66 - 3 \cdot 42 \\ &= 2 \cdot 66 - 3 \cdot (108 - 66) = 5 \cdot 66 - 3 \cdot 108 \\ &= 5 \cdot (606 - 108 \cdot 5) - 3 \cdot 108 = 5 \cdot 606 - 28 \cdot 108. \end{aligned}$$

Es decir, $6 = 5 \cdot 606 - 28 \cdot 108$.

20. Probar que no existen enteros x e y que satisfagan $x + y = 100$ y $(x, y) = 3$.
    Rta: Si $(x, y) = 3$ entonces $3|x, 3|y$ y por lo tanto $3|x + y = 100$, absurdo.

21. *a*) Sean a y b coprimos. Probar que si $a \mid b \cdot c$ entonces $a \mid c$.
    Rta: Como a y b son coprimos, existen $r, s \in \mathbb{Z}$ tales que $1 = ra + sb$, por lo tanto $c = rac + sbc$ y como a divide ambos sumandos, $a \mid c$.

    b) Sean a y b coprimos. Probar que si $a \mid c$ y $b \mid c$, entonces $a \cdot b \mid c$.
    Rta: Como a y b son coprimos, existen $r, s \in \mathbb{Z}$ tales que $1 = ra + sb$. Además, $ap = c = bq$, con $p, q \in \mathbb{Z}$, entonces $c = rac + sbc = rabq + sbap = (rq + sp)ab$. Por lo tanto, $a \cdot b \mid c$.

22. Probar que si $n \in \mathbb{Z}$, entonces los números $2n + 1$ y $\dfrac{n(n+1)}{2}$ son coprimos.
    Rta: Tenemos que $d = \left(2n + 1, \frac{n(n+1)}{2}\right) \geq 1$. Si $d > 1$, entonces existe un primo p tal que $p \mid d$, por tanto $p \mid (2n + 1)$ y $p \mid \frac{n(n+1)}{2}$. Ahora, si p divide a $\frac{n(n+1)}{2}$, p debe dividir a $n(n + 1)$ y por ser primo debe dividir a n ó a $n + 1$. Como se pide que $p \mid (2n + 1)$, entonces ambos casos implican que $p \mid 1$, lo cual es absurdo. De donde, $d = 1$.
    Rta Alternativa: Si $(a, b) = 1$ y $(a, c) = 1$ entonces $(a, b \cdot c) = 1$, ya que un primo que divida a $b \cdot c$ debe dividir a b ó a c y entonces no puede dividir a a. Como $(2n + 1, n) = 1 = (2n + 1, n + 1)$ entonces $(2n + 1, n(n + 1)) = 1$ y por lo tanto $2n + 1$ es coprimo con $\frac{n(n+1)}{2}$.
    Observación: $1 = (2n + 1)(2n + 1) - 8\frac{n(n+1)}{2} \iff \left(2n + 1, \frac{n(n+1)}{2}\right) = 1.$

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

Rta: Es claro que $\left(\frac{a}{10},\frac{b}{10}\right) = 1$ y $\left[\frac{a}{10},\frac{b}{10}\right] = 10$. Pero,

$$\left[\frac{a}{10},\frac{b}{10}\right] = \frac{\left(\frac{a}{10}\right)\cdot\left(\frac{b}{10}\right)}{\left(\frac{a}{10},\frac{b}{10}\right)} = \left(\frac{a}{10}\right)\cdot\left(\frac{b}{10}\right)$$

Por lo tanto $\left(\frac{a}{10}\right)\cdot\left(\frac{b}{10}\right) = 10$, y como $10 = 1\cdot 10 = 10\cdot 1 = 2\cdot 5 = 5\cdot 2$, se sigue que: $a = 10, b = 100$ ó $a = 100, b = 10$ ó $a = 20, b = 50$ ó $a = 50, b = 20$.

24. *a*) Probar que si d es divisor común de a y b, entonces $\frac{(a,b)}{d} = \left(\frac{a}{d},\frac{b}{d}\right)$.

    Rta: Existen $p, q \in \mathbb{Z}$ tales que $a = dp$ y $b = dq$. Luego, $\frac{a}{d} = p$ y $\frac{b}{d} = q$. De donde,

    $$\frac{(a,b)}{d} = \frac{(dp,dq)}{d} = \frac{d(p,q)}{d} = (p,q) = \left(\frac{a}{d},\frac{b}{d}\right).$$

    b) Probar que si $a, b \in \mathbb{Z}$ no nulos, entonces $\frac{a}{(a,b)}$ y $\frac{b}{(a,b)}$ son coprimos.

    Rta: usar el inciso anterior con $d = (a,b)$.

25. Probar que 3 y 5 son números primos.

    Rta: 3 no es divisible por 2 y 5 no es divisible por 2 ni por 3.

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

    Rta: 2,3,5,7, están en la lista. Por el criterio de la raíz debemos ver cuales números del 8 al 100 no son divisibles por 2, 3, 5 ni 7. Estos son: 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

27. Determinar con el criterio de la raíz cuáles de los siguientes números son primos: 113, 123, 131, 151, 199, 503.

    Rta: $\sqrt{113} < 11$ y 113 no es divisible por 2, 3, 5 y 7, por lo tanto es primo. $123 = 3\cdot 41$ luego no es primo. 131 es primo, pues $\sqrt{131} < 12$ y 131 no es divisible por 2, 3, 5, 7 y 11. 151 es primo, pues $\sqrt{151} < 13$ y 151 no es divisible por 2, 3, 5, 7 y 11. 199 es primo, pues $\sqrt{199} < 15$ y 199 no es divisible por 2, 3, 5, 7, 11 y 13. 503 es primo, pues $\sqrt{503} \sim 22{,}42... < 23$ y 503 no es divisible por 2, 3, 5, 7, 11, 13, 17 y 19.

28. Si $a \cdot b$ es un cuadrado y a y b son coprimos, probar que a y b son cuadrados.
Rta: Sean $a, b \in \mathbb{N} \cup \{0\}$ tales que $(a, b) = 1$. Podemos asumir que $a > 1$ y $b > 1$, ya que si alguno es cero (no ambos) ó alguno es uno (pueden ser ambos) el resultado se cumple.
Luego, $a = \prod_{i=1}^{r} p_i^{m_i}$ y $b = \prod_{i=1}^{s} q_i^{n_i}$, donde $r, s, m_i, n_i \in \mathbb{N}$; p_i y q_i son primos (distintos entre sí) positivos tales que $p_i \neq q_j$ para todo i, j (pues $(a, b) = 1$). Por lo tanto, la factorización de $a \cdot b$ es $a \cdot b = p_1^{m_1} \cdots p_r^{m_r} \cdot q_1^{n_1} \cdots q_s^{n_s}$.
Ahora, supongamos que $a \cdot b$ es un cuadrado, digamos $a \cdot b = c^2$. Se sigue que $a \cdot b$ y c tienen los mismos factores primos (los divisores primos de c^2, son divisores primos de c), y por lo tanto c tendrá una factorización de la forma $c = p_1^{c_1} \cdots p_r^{c_r} \cdot q_1^{d_1} \cdots q_s^{d_s}$, con $c_i, d_i \in \mathbb{N}$. Así,
$$a \cdot b = c^2 = p_1^{2c_1} \cdots p_r^{2c_r} \cdot q_1^{2d_1} \cdots q_s^{2d_s}$$
De donde, por la unicidad de la factorización: $m_i = 2c_i$, $n_j = 2d_j$ para todo i, j $\Longrightarrow$ a y b son cuadrados.

29. Probar que si p_k es el k-ésimo primo positivo entonces
$$p_{k+1} \leq p_1 \cdot p_2 \cdots p_k + 1$$
Rta: el miembro de la derecha no es divisible por ninguno de los primeros k primos, luego o es el $(k+1)$-ésimo primo, o es divisible por un primo mayor que este. Por lo tanto, debe ser un número mayor o igual que el $(k+1)$-ésimo primo.

30. *a*) Probar que $\sqrt{5}$ no es un número racional.
Rta: Supongamos que $\sqrt{5}$ es racional, es decir $\sqrt{5} = \dfrac{n}{m}$ con $n \in \mathbb{Z}$, $m \in \mathbb{N}$, luego $5 = \sqrt{5}^2 = \dfrac{n^2}{m^2}$ y haciendo pasaje de término obtenemos $5m^2 = n^2$. Sea $m = 5^r m_1$ y $n = 5^s n_1$ donde m_1, n_1 no tienen el primo 5 en su descomposición en factores primos (es decir $(5, m_1) = (5, n_1) = 1$), y $r \in \mathbb{N} \cup \{0\}$, $s \in \mathbb{N}$. Luego $5m^2 = 5 \cdot 5^{2r} m_1^2 = 5^{2r+1} m_1^2$ y $n^2 = 5^{2s} n_1^2$, y por lo tanto $5^{2r+1} m_1^2 = 5^{2s} n_1^2$. Por la unicidad de la escritura en la descomposición prima, tenemos que $2r + 1 = 2s$, lo cual es absurdo. El absurdo vino de suponer que $\sqrt{5}$ es un número racional.
b) Probar que $\sqrt{15}$ no es un número racional.

Rta: Como en el ejercicio anterior debemos ver que $15m^2 = n^2$ nos lleva a un absurdo. Ahora bien, si $m = 5^r m_1$ y $n = 5^s n_1$ con 5 coprimo con m_1 y n_1, y $r \in \mathbb{N} \cup \{0\}$, $s \in \mathbb{N}$, tenemos que $5^{2r+1} 3m_1^2 = 5^{2s} n_1^2 \Rightarrow 2r + 1 = 2s$, absurdo.

c) Probar que $\sqrt{8}$ no es un número racional.

Rta: En este caso suponemos que $\sqrt{8} = n/m$, luego $8m^2 = n^2$. Si $m = 2^r m_1$ y $n = 2^s n_1$ con $(2, m_1) = (2, n_1) = 1$, tenemos que $2^3 \cdot 2^{2r} m_1^2 = 2^{2s} n_1^2$, por lo tanto $2^{2r+3} m_1^2 = 2^{2s} n_1^2$. Luego $2r + 3 = 2s$ lo cual es absurdo pues un impar no puede ser igual a un par.

d) Probar que $\sqrt[3]{4}$ no es un número racional.

Rta: Si fuera racional tendríamos $\sqrt[3]{4} = n/m$ y por lo tanto (elevando al cubo) $4 = n^3/m^3$, o equivalentemente, $2^2 m^3 = n^3$. Si $m = 2^r m_1$ y $n = 2^s n_1$ con $(2, m_1) = (2, n_1) = 1$, tenemos $2^2 m^3 = 2^2 \cdot 2^{3r} m_1^3 = 2^{3r+2} m_1^3$ y $n^3 = 2^{3s} n_1^3$. Por lo tanto $3r + 2 = 3s$ lo cual es absurdo, pues $3r + 2$ no es múltiplo de 3 y $3s$ sí lo es.

31. Calcular el máximo común divisor y el mínimo común múltiplo de los siguientes pares de números usando la descomposición en números primos.

Recordar: Si $a = \prod_{i=1}^{r} p_i^{m_i}$ y $b = \prod_{i=1}^{r} p_i^{n_i}$, entonces

$$(a, b) = \prod_{i=1}^{r} p_i^{k_i} \quad \text{y} \quad [a, b] = \prod_{i=1}^{r} p_i^{h_i}$$

donde para todo $1 \leq i \leq r$, $k_i = \min\{m_i, n_i\}$ y $h_i = \max\{m_i, n_i\}$.

a) $a = 12$ y $b = 15$. *Rta:* $a = 2^2 \cdot 3$, $b = 3 \cdot 5$, $(a, b) = 3$, $[a, b] = 2^2 \cdot 3 \cdot 5$.

b) $a = 11$ y $b = 13$. *Rta:* $(a, b) = 1$, $[a, b] = 11 \cdot 13 = 143$.

c) $a = 140$ y $b = 150$. *Rta:* $a = 2^2 \cdot 5 \cdot 7$, $b = 2 \cdot 3 \cdot 5^2$, $(a, b) = 2 \cdot 5 = 10$, $[a, b] = 2^2 \cdot 3 \cdot 5^2 \cdot 7 = 2100$

d) $a = 3^2 \cdot 5^2$ y $b = 2^2 \cdot 11$. *Rta:* $(a, b) = 1$, $[a, b] = 2^2 \cdot 3^2 \cdot 5^2 \cdot 11$

e) $a = 2^2 \cdot 3 \cdot 5$ y $b = 2 \cdot 5 \cdot 7$. *Rta:* $(a, b) = 2 \cdot 5$, $[a, b] = 2^2 \cdot 3 \cdot 5 \cdot 7$.