55. $A = (\mathbb{Z} - \{0\}) \times (\mathbb{Z} - \{0\})$

$(a,b)\,R\,(c,d) \Leftrightarrow ad = bc$ on $a,b,c,d \in A$

1) Reflexiva $(a,b)\,R\,(a,b) \Leftrightarrow ab = ba \Leftrightarrow ab = ab$

Simètrica $(a,b)\,R\,(c,d) \Leftrightarrow ad = bc \Leftrightarrow bc = ad \Leftrightarrow (c,d)\,R\,(a,b)$

Transitiva $(a,b)\,R\,(c,d) \wedge (c,d)\,R\,(e,f) \Leftrightarrow \begin{matrix} ad = bc \\ cf = de \end{matrix} \Leftrightarrow adf = bcf = bde \Leftrightarrow af = bcf = be$

$\Leftrightarrow af = be \Leftrightarrow (a,b)\,R\,(e,f)$

2) $\overline{(a,b)} = \{(x,y) : ay = bx\}$

3) $A/R = \{\overline{(a,b)} : (a,b) \in A\}$

86. $\mathbb{R} \times \mathbb{R}$

$(x,y)\,R\,(z,t) \Leftrightarrow |x| + |y| = |z| + |t|$

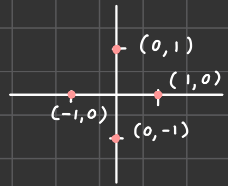
1) Reflexiva $(x,y)\,R\,(x,y) \Leftrightarrow |x| + |y| = |x| + y|$

Simètrica $(x,y)\,R\,(z,t) \Leftrightarrow |x| + |y| = |z| + |t| \Leftrightarrow |z| + |t| = |x| + |y| \Leftrightarrow (z,t)\,R\,(x,y)$

Transitiva $(x,y)\,R\,(z,t) \wedge (z,t)\,R\,(a,b) \Leftrightarrow |x| + |y| = |z| + |t| = |a| + |b| \Leftrightarrow (x,y)\,R\,(a,b)$

2) Elements classe $(1,0)$

$\overline{(1,0)} = \{(x,y) \cdot (x,y)\,R\,(1,0) \Rightarrow |x| + |y| = 1\} = \{\overline{(0,1)}, \overline{(1,0)}, \overline{(0,-1)}, \overline{(-1,0)}\}$



124. $A = \mathbb{Z} - \{0\}$

$mRn \Leftrightarrow$ (signe (n) = signe (m) $\wedge$ paritat (n) = paritat (m)) $\vee$
(signe $(n) \neq$ signe (m) $\wedge$ paritat $(n) \neq$ paritat (m))

1) Reflexiva $nRn \Leftrightarrow$ signe (n) = signe (n) $\wedge$ paritat (n) = paritat (n)

Simètrica $nRm \Leftrightarrow$ signe (n) = signe (m) $\wedge$ paritat (n) = paritat (m) $\Leftrightarrow$ signe (m) = signe (n) $\wedge$ paritat (m) = paritat (n) $\Leftrightarrow mRn$

Transitiva $nRm \wedge mRx$

a) $nRm \wedge mRx \Leftrightarrow$ signe (n) = signe (m) = signe (x) $\wedge$ paritat (n) = paritat (m) = paritat (x) $\Leftrightarrow nRx$

b) $nRm \wedge mRx \Leftrightarrow$ signe (n) = signe $(m) \neq$ signe (x) $\wedge$ paritat (n) = paritat $(m) \neq$ paritat (x) $\Leftrightarrow nRx$

c) $nRm \wedge mRx \Leftrightarrow$ signe $(n) \neq$ signe (m) = signe (x) $\wedge$ paritat $(n) \neq$ paritat (m) = paritat (x) $\Leftrightarrow nRx$

d) $nRm \wedge mRx \Leftrightarrow$ signe (n) = signe $(x) \neq$ signe (m) $\wedge$ paritat (n) = paritat $(x) \neq$ paritat (x) $\Leftrightarrow nRx$

2) classe d'equivalència 1 i 2

$\bar{1} = \{x \in A : xR1\} = \{\bar{3}, \bar{5}, \bar{7}, \dots\} \cup \{-\bar{2}, -\bar{4}, -6, \dots\}$

$\bar{2} = \{x \in A : xR2\} = \{\bar{4}, \bar{6}, \bar{8}, \dots\} \cup \{-\bar{1}, -\bar{3}, -\bar{5}, \dots\}$

3) $A/R = \{\bar{1}, \bar{2}\}$

217. $n \geq 2$, $X = \{0,1\}^n$

$x_1 x_2 \dots x_n \,R\, y_1, y_2 \dots y_n \Leftrightarrow x_1 = y_1 \wedge x_2 = y_2$

a) Reflexiva $x_1 x_2 \dots x_n \,R\, x_1 x_2 \dots x_n \Leftrightarrow x_1 = x_1 \wedge x_2 = x_2$

Simètrica $x_1 x_2 \dots x_n \,R\, y_1 y_2 \dots y_n \Leftrightarrow x_1 = y_1 \wedge x_2 = y_2 \Leftrightarrow y_1 = x_1 \wedge y_2 = x_2 \Leftrightarrow y_1 y_2 \dots y_n \,R\, x_1 x_2 \dots x_n$

Transitiva $x_1 x_2 \dots x_n \,R\, y_1 y_2 \dots y_n \wedge y_1 y_2 \dots y_n \,R\, z_1 z_2 \dots z_n \Leftrightarrow x_1 = y_1 = z_1 \wedge x_2 = y_2 = z_2 \Leftrightarrow x_1 x_2 \dots x_n \,R\, z_1 z_2 \dots z_n$

b) Classe d'equivalencia (binari)

$\overline{(x_1 x_2 \dots x_n)} = \{y_1 y_2 \dots y_n \in X : x_1 = y_1 \wedge x_2 = y_2\}$

$\overline{(00\dots0)} = \{y_1 y_2 \dots y_n \in X : y_1 = 0 \wedge y_2 = 0\}$

$\overline{(01\dots0)} = \{y_1 y_2 \dots y_n \in X : y_1 = 0 \wedge y_2 = 1\}$

$\overline{(10\dots0)} = \{y_1 y_2 \dots y_n \in X : y_1 = 1 \wedge y_2 = 0\}$

$\overline{(11\dots0)} = \{y_1 y_2 \dots y_n \in X : y_1 = 1 \wedge y_2 = 1\}$

c) conjunt cocient

$X/R = \{ (\overline{00\ldots0}), (\overline{01\ldots0}), (\overline{10\ldots0}), (\overline{11\ldots0}) \}$

339. $\mathbb{Z} \times \mathbb{Z}$

$(x,y) R (x',y') \Leftrightarrow x-x'$ parell $\wedge$ $y-y'$ parell

a) Reflexiva $(x,y) R (x,y) \Leftrightarrow$ $x-x$ parell $\wedge$ $y-y$ parell , 0 parell $\wedge$ 0 parell

Simètrica $(x,y) R (x',y') \Leftrightarrow \exists k,t \in \mathbb{Z}$ tq $x-x' = 2k \wedge y-y' = 2t \Leftrightarrow x'-x = 2(-k) \wedge y'-y = 2(-t)$

$\Leftrightarrow (x',y') R (x,y)$

Transitiva $(x,y) R (x',y') \wedge (x',y') R (x'',y'') \Leftrightarrow \exists k,t,n,m \in \mathbb{Z}$ tq $x-x' = 2k \wedge y-y' = 2t$

$\wedge\ x'-x'' = 2n \wedge y'-y'' = 2m \Leftrightarrow x-x'' = (x-x') + (x'-x'') = 2k+2n = 2(k+n) \wedge$

$y-y'' = (y-y') + (y'-y'') = 2t+2m = 2(t+m) \Leftrightarrow (x,y) R (x'',y'')$

b) Classe d'equivalència

$(\overline{x,y}) = \{ (a,b) \in \mathbb{Z} : (x,y) R (a,b) \rightarrow \exists k,t \in \mathbb{Z}$ tq $x-a = 2k \wedge y-b = 2t \}$

* (x,y) parell $(\overline{0,0})$
* (x,y) senar $(\overline{1,1})$
* x parell , y senar $(\overline{0,1})$
* x senar, y parell $(\overline{1,0})$

c) $\mathbb{Z}/R = \{ (\overline{0,0}), (\overline{0,1}), (\overline{1,0}), (\overline{1,1}) \}$

353. $\mathbb{R}$

$aRb \Leftrightarrow \lceil a+1 \rceil = \lceil b+1 \rceil$

a) Reflexiva $aRa \Leftrightarrow \lceil a+1 \rceil = \lceil a+1 \rceil$

Simètrica $aRb \Leftrightarrow \lceil a+1 \rceil = \lceil b+1 \rceil \Leftrightarrow \lceil b+1 \rceil = \lceil a+1 \rceil \Leftrightarrow bRa$

Transitiva $aRb \wedge bRc \Leftrightarrow \lceil a+1 \rceil = \lceil b+1 \rceil = \lceil c+1 \rceil \Leftrightarrow aRc$

b) Classes d'equivalència de π, $-\pi$, x.

$\overline{\pi} = \{ x \in \mathbb{R} : \lceil \pi+1 \rceil = \lceil x+1 \rceil \} = (\overline{3,4}]$

$\lceil \pi+1 \rceil = 5$; $5 = x+1$; $x = 4$

$-\overline{\pi} = \{ x \in \mathbb{R} : \lceil -\pi+1 \rceil = \lceil x+1 \rceil \} = (\overline{-4,-3}]$

$\overline{x} = \{ k \in \mathbb{R} : \lceil x+1 \rceil = \lceil k+1 \rceil \} = (\overline{k, k+1}]$

c) conjunt cocient

$\mathbb{R}/R = \{ \overline{x} : x \in \mathbb{R} \longrightarrow (k, k+1] : k \in \mathbb{R} \}$

17. $f : \mathbb{N} \rightarrow \mathbb{N}$

$f(n) = \begin{cases} n & n \text{ parell} \\ n+1 & n \text{ senar} \end{cases}$

1) $f \circ f = f$?

n parell $\Rightarrow f(f(n)) = f(n) = n$

n senar $\Rightarrow f(f(n)) = f(n+1) \Rightarrow n$ senar $+1 =$ parell $\Rightarrow f(n+1) = n+1$

Per tant $f \circ f = f$ cvd.

2) $f[\{1,2,3,4\}]$. Dedueix f no injectiva

$f[\{1,2,3,4\}] = \{2,4\}$

f injectiva $\Rightarrow \forall x, x' \in \mathbb{N} \,(f(x) = f(x') \rightarrow x = x') \Rightarrow$ contra exemple $f(1) = f(2) \wedge 1 \neq 2$.

3) $f^{-1}[\{0,1,2\}] = \{0,2\}$

$f^{-1}(n) = \begin{cases} n & n \text{ parell} \\ n-1 & n \text{ senar} \end{cases}$ Els senars no tenen antimatge per tant no és exhaustiva

19. $f: \mathbb{Z} \to \mathbb{Z}$

$$f(n) = \begin{cases} -n^2 & \text{si } n<0 \\ n^2 & \text{si } n \geq 0 \end{cases}$$

1) $f[\{-2,-1,0,1,2\}] = \{-4,-1,0,1,4\}$

2) f injectiva $\Rightarrow \forall n, n' \in \mathbb{Z}\,(f(n) = f(n') \to n=n')$

$f(n) = f(n') \Rightarrow \quad n^2 = n'^2 \vee n^2 = -n'^2 \Rightarrow \quad n^2 - n'^2 = 0 \quad \vee \quad n^2 + n'^2 = 0$

$$\begin{cases} n^2 + n'^2 = 0 \Rightarrow n = n' = 0 \\ n^2 - n'^2 = 0 \Rightarrow (n-n')(n+n') = 0 \Rightarrow n - n' = 0 \Rightarrow n = n' \end{cases}$$

3) $f^{-1}[\{0,1,2\}] = \{0,1\}$ el 2 no té antimatge ja que $f: \mathbb{Z} \to \mathbb{Z}$

$y = -n^2 \Rightarrow n = -\sqrt{y}$

$y = n^2 \Rightarrow n = \sqrt{y}$

f no és exhaustiva.

21. $f: \mathbb{N} \to \mathbb{Z}$

$$f(n) = \begin{cases} -n/2 & \text{si } n \text{ parell} \\ \frac{n+1}{2} & \text{si } n \text{ senar} \end{cases}$$

1) calcula $f[\{0,1,2,3,4,5\}] = \{0,1,-1,2,-2,3\}$

$f[\{0,3,5,6,7,10\}] = \{0,2,3,-3,4,-5\}$

2) calcula

$$f^{-1}(n) = \begin{cases} -2n & n \text{ negatiu} \\ 2n-1 & n \text{ positiu} \end{cases}$$

$f^{-1}[\{-1,0,1,2\}] = \{2,0,1,3\}$

$f^{-1}[\{-3,-1,0,1\}] = \{6,2,0,1\}$

3) f exhaustiva?

$\forall y \in \mathbb{Z}\ \exists x \in \mathbb{N}$ tq $f(x) = y$

si $y \geq 0 \quad y = 2x-1$ és exhaustiva

si $y < 0 \quad y = -2x$

4) f injectiva?

$f(n) = f(n') \Leftrightarrow n = n'$

n, n' parell $\Rightarrow -\frac{n}{2} = -\frac{n'}{2} \Rightarrow n = n'$

és injectiva

n, n' senar $\Rightarrow \frac{n+1}{2} = \frac{n'+1}{2} \Rightarrow n = n'$

103. * $f: \mathbb{N} \to \mathbb{N}$ injectiva

Prova que $g: \mathbb{N} \to \mathbb{N}$ $g(n) = 2f(n)$ és injectiva

$g(n) = g(n') \Rightarrow \cancel{2}f(n) = \cancel{2}f(n') \Rightarrow f(n) = f(n') \Rightarrow f(n)$ és injectiva $\Rightarrow n = n'$ per tant, conseqüentment $g(n)$ també.

* Descriu $P(P(\emptyset)) \Rightarrow P(\emptyset) = \{\emptyset\} \Rightarrow P(P(\emptyset)) = \{\emptyset, \{\emptyset\}\}$

203. $f: \mathbb{Z}_{400} \to \mathbb{Z}_{400}$

$$f(\bar{x}) = \begin{cases} \bar{7}\bar{x} + \bar{1} & \text{si } \bar{x} \in \{\bar{0}, \bar{2}, \dots, \overline{398}\} \quad \text{parells} \\ \bar{4}\bar{x} + \bar{3} & \text{si } \bar{x} \in \{\bar{1}, \bar{3}, \dots, \overline{399}\} \quad \text{senars} \end{cases}$$

a) f injectiva? $\quad f(n) = f(n') \Leftrightarrow n = n'$

* per n, n' parells: $\bar{7}\bar{n} + \cancel{\bar{1}} = \bar{7}\bar{n}' + \cancel{\bar{1}} \Rightarrow \bar{7}\bar{n} = \bar{7}\bar{n}'$ $\quad mcd(7,400) = 1 \ \exists \bar{7}^{-1}$
$\Rightarrow \bar{n} = \bar{n}'$
* Per n, n' senars: $\bar{4}\bar{n} + \cancel{\bar{3}} = \bar{4}\bar{n}' + \cancel{\bar{3}} \Rightarrow \bar{4}\bar{n} = \bar{4}\bar{n}'$ $mcd(4,400) \neq 1 \ \nexists \bar{4}^{-1}$ no puc concluir que $n = n'$.

$f(x)$ no és injectiva

b) $f(x)$ exhaustiva? Els nombres parells no tenen imatge per tant $f(x)$ no és exhaustiva.

c) $f^{-1}[\{\overline{201}\}]$?

$\overline{201} = \bar{7}\bar{x} + \bar{1} \Rightarrow \bar{7}\bar{x} = \overline{200}$ $\quad mcd(7,400) = 1 \ \exists \bar{7}^{-1} \Rightarrow \bar{x} = \bar{7}^{-1} \Rightarrow \bar{x} = \overline{343} \Rightarrow$
$\Rightarrow \bar{7} \cdot \overline{343} \overset{?}{=} \overline{200} \Rightarrow \overline{68600} \overset{?}{=} \overline{200} \Rightarrow \overline{200} = \overline{200}$ cert

$f^{-1}[\{\overline{201}\}] = \overline{200}$

232 $\quad f, g: \mathbb{Z} \to \mathbb{Z}$

$$f(n) = \begin{cases} n^2 & n \text{ parell} \\ (n-1)^2 & n \text{ senar} \end{cases} \qquad g(n) = \begin{cases} 3n & n \text{ parell} \\ 3n+1 & n \text{ senar} \end{cases}$$

a) $\forall n \in \mathbb{Z} \to (g \circ f)(n) = 3f(n)$

$(g \circ f)(n) \Rightarrow g(f(n)) = \begin{cases} 3n^2 & n \text{ parell} \\ 3(n-1)^2 + 1 & n \text{ senar} \end{cases} \Rightarrow g(f(n)) = \begin{cases} 3n^2 \\ 3(n-1)^2 \end{cases} = 3f(n)$

b) f injectiva? $\quad f(n) = f(n') \Longrightarrow n = n'$

Contraexemple $\Rightarrow \begin{matrix} f(4) = 4^2 = 16 \\ f(5) = (5-1)^2 = 16 \end{matrix} \Rightarrow 4 \neq 5 \Rightarrow f$ no és injectiva

c) g exhaustiva? $\quad \forall y \in \mathbb{Z} \ \exists x \in \mathbb{Z}$ tq $f(x) = y$

n parell $\Rightarrow y = 3n \Rightarrow n = \frac{y}{3} \Rightarrow f^{-1}(n) = \frac{n}{3}$ tots aquells enters que no siguin divisibles per 3 no tenen imatge, per tant, g no és exhaustiva.

d) $T = \{3k : k \in \mathbb{Z}\}$. Calcula $f[g^{-1}[T]]$
Com que tots els elements de te són $3k \Rightarrow 3 \mid 3k \Rightarrow$ tots tindran imatge.

$g^{-1}[T] = \{n \in \mathbb{Z} : g(n) \in T\}$

Hem de trovar els enters que compleixin $g(n) = 3k \Rightarrow n$ parell $\Rightarrow$
$g(n) = \cancel{3}n = \cancel{3}k \Rightarrow n = k \Rightarrow$ per k parell. $\Rightarrow g^{-1}[T] = \{2t : t \in \mathbb{Z}\}$
$\Rightarrow f[g^{-1}[T]] = \{4t^2 : t \in \mathbb{Z}\}$

278. $a \in \mathbb{Z}$. $f_a : \mathbb{Z}_{100} \to \mathbb{Z}_{100}$
$f_a(\bar{x}) = \bar{a}\bar{x} + \bar{4}$

a) si $mcd(a, 100) = 1 \Rightarrow f_a$ bijectiva

f_a bijectiva $\Leftrightarrow f_a$ injectiva $\wedge f_a$ exhaustiva

* f_a injectiva : $f(\bar{x}) = f(\bar{x}') \Leftrightarrow \bar{x} = \bar{x}' \Rightarrow \bar{a}\bar{x} + \cancel{\bar{4}} = \bar{a}\bar{x}' + \cancel{\bar{4}} \Rightarrow \bar{a}\bar{x} = \bar{a}\bar{x}$

$\Rightarrow$ si $mcd(a, 100) = 1 \Rightarrow \exists \bar{a}^{-1} \Rightarrow \bar{a}\cdot\bar{a}^{-1} = \bar{1} \Rightarrow \bar{x} = \bar{x}'$.

* f_a exhaustiva : $\forall \bar{y} \in \mathbb{Z}_{100}\ \exists \bar{x} \in \mathbb{Z}_{100}$ tq $f(\bar{x}) = \bar{y}$. $\Rightarrow \bar{y} = \bar{a}\bar{x} + \bar{4} \Rightarrow \bar{y} - \bar{4} = \bar{a}\bar{x}$

$\Rightarrow$ si $mcd(a, 100) = 1 \Rightarrow \exists \bar{a}^{-1} \Rightarrow \bar{a}\cdot\bar{a}^{-1} = \bar{1} \Rightarrow (\bar{y} - \bar{4})\bar{a}^{-1} = \bar{x} \Rightarrow f^{-1}(\bar{x}) = (\bar{x} - \bar{4})\bar{a}^{-1}$.

b) f_{77}. calcula $f_{77}^{-1}[\{30\}]$

$mcd(77, 100) = 1 \Rightarrow f_{77}$ bijectiva $\Rightarrow \exists f_{77}^{-1}(x)$. $\Rightarrow f_{77}^{-1}(\bar{x}) = \overline{77}^{-1} \cdot (\bar{x} - \bar{4}) \Rightarrow$

	0	1	-1	4	-9	13
c		1	3	2	1	7
r	100	77	23	8	7	1

$\overline{77}^{-1} = \overline{13} \Rightarrow f_{77}^{-1}(\bar{x}) = \overline{13}(\bar{x} - \bar{4}) \Rightarrow f_{77}^{-1}(\overline{30}) = \overline{13}\cdot(\overline{30} + \overline{48}) = \overline{38}$

$\Rightarrow f_{77}^{-1}[\{\overline{30}\}] = \{\overline{38}\}$

c) f_{55} ni injectiva ni exhaustiva $\Rightarrow f_a$ es injectiva i exhaustiva si només si $mcd(a, 100) = 1 \Rightarrow mcd(55, 100) = 5 \neq 1$ per tant f_{55} no ho és.

301. $A = \{0, 1, 2, 3\}$

a) $P(A) = \{\emptyset, \{0\}, \{1\}, \{3\}, \{0,1\}, \{0,2\}, \{0,3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{0,1,2\},$
$\{0,1,3\}, \{0,2,3\}, \{1,2,3\}, A\}$

b) $f : P(A) \to P(A)$. $f(x) = (x \setminus \{0\}) \cup \{1\}$. f injectiva ? f exhaustiva?

* $f[\{0\}] \wedge f[\{1\}] = \{1\}$ per tant f no és injectiva
* $\emptyset$ no té anti imatge per tant f no és exhaustiva

338. $f : \mathbb{R} - \{2\} \to \mathbb{R} - \{2\}$.
$f(x) = \dfrac{2x+1}{x-2}$

a) f ben definida?

$\mathbb{R} - \{2\} \Rightarrow x - 2 = 0 \Rightarrow x = 2$. ✓

$\Rightarrow \dfrac{2x+1}{x-2} = 2 \Rightarrow \cancel{2x} + 1 = \cancel{2x} - 4 \Rightarrow 1 \neq -4$. ✓

b) f injectiva $\Rightarrow f(x) = f(x') \Rightarrow x = x' \Rightarrow \dfrac{2x+1}{x'-2} = \dfrac{2x'+1}{x'-2} \Rightarrow (2x+1)(x'-2) = (2x'+1)(x-2)$

$\Rightarrow \cancel{2x}x' - 4x + x' - \cancel{2} = \cancel{2x'}x - 4x' + x - \cancel{2} \Rightarrow \cancel{5}x = \cancel{5}x' \Rightarrow x = x'$.

c) f exhaustiva $\Rightarrow \forall y \in \mathbb{R} - \{2\}\ \exists x \in \mathbb{R} - \{2\}$ tq $f(x) = y \Rightarrow y = \dfrac{2x+1}{x-2} \Rightarrow y(x-2) = 2x+1$

$\Rightarrow yx - 2y = 2x + 1 \Rightarrow yx - 2x = 2y + 1 \Rightarrow x(y-2) = 2y + 1 \Rightarrow x = \dfrac{2y+1}{y-2}$

per $x \neq 2$ i $y \neq 2$.

d) Justifica que $\exists f^{-1}$, calcula-la.

f bijectiva $\Leftrightarrow \exists f^{-1}$ per tant f té inversa.

$x = \dfrac{2y+1}{y-1} \Rightarrow f^{-1}(x) = \dfrac{2x+1}{x-2}$

e) $g = f\circ f$. g bijectiva? g^{-1}?

$$g = f\circ f = f(f(x)) = f\left(\frac{2x+1}{x-2}\right) = \frac{2\left(\frac{2x+1}{x-2}\right)+1}{\left(\frac{2x+1}{x-2}\right)-2} = \frac{2(2x+1)+(x-2)}{2(2x+1)-2(x-2)} = \frac{5x}{5} = x.$$

com que $g = f\circ f = f\circ f^{-1} = I_{\mathbb{R}-\{2\}} \Rightarrow g$ bijectiva

42. $a,b \in \mathbb{Z}$ i $d = \text{mcd}(a,b) \Rightarrow \text{mcd}(2a,d) = d$

$d = \text{mcd}(a,b) \Rightarrow d \mid a \wedge d \mid b \Rightarrow d \mid 2a \wedge d \mid d \Rightarrow \text{mcd}(2a,d) = d$

50. $a,b \in \mathbb{Z}$. $\text{mcd}(a,b) \mid \text{mcd}(a, a+b)$

Teorema d'Euclides $\Rightarrow \text{mcd}(a+b, a) = \text{mcd}(a+b-a, a) = \text{mcd}(a,b) \Rightarrow$

$\Rightarrow \text{mcd}(a,b) = |ab| \cdot \text{mcd}(a,b)$

61. $a,b,c \in \mathbb{Z} \Rightarrow \text{mcd}(a,b) = \text{mcd}(bc-a, b)$

$\text{mcd}(a,b) = d$

$\text{mcd}(bc-a, b) = k$ $\Rightarrow d \mid k \wedge k \mid d$

$\text{mcd}(a,b) = d \Rightarrow d \mid a \wedge d \mid b \Rightarrow$ per linealitat $d \mid bc-a$ per $c \in \mathbb{Z} \Rightarrow d \mid k$

$\text{mcd}(bc-a, b) = k \Rightarrow k \mid bc-a \wedge k \mid b \Rightarrow$ per linealitat $k \mid (bc-(bc-a)) \Rightarrow k \mid a \wedge k \mid b \Rightarrow k \mid d$.

89. 1) $\text{mcd}(1876, 365) = 1$. calcula $1876r + 365s = 1$

Algorisme d'Euclides

1	0	1	-7	43	-93	136
0	1	-5	36	-221	478	-699
	5	7	6	2	1	2
1876	365	51	8	3	2	1

$1876 \cdot (136) + 365(-699) = 1$

2) x mínima tal que $365x + 902 \equiv -508 \pmod{1876}$

$\overline{365}\,\overline{x} + \overline{902} = -\overline{508} \Rightarrow \overline{365}\,\overline{x} = \overline{466} \Rightarrow \text{mcd}(365, 1876) = 1 \; \exists\, \overline{365}^{-1} = -\overline{699} = \overline{1177}$

$\Rightarrow \overline{x} = \overline{466} \cdot \overline{1177} = \overline{690} \Rightarrow x = 690.$

127. 1) Prova que $\exists\, \overline{2957}^{-1}$ en $\mathbb{Z}_{4096}$ i calcula-ho.

$\text{mcd}(2957, 4096) = 1$ per tant $\exists\, \overline{2957}^{-1} \Rightarrow$ Id Bezout $\text{mcd}(2957, 4096) = 2957\alpha + 4096\beta$

Algorisme d'Euclides

0	1	-1	3	-4	7	-18	169	-187
	1	2	1	1	2	9	1	0
4096	2957	1139	679	460	219	22	21	1

$\overline{2957}^{-1} = -\overline{187} = \overline{3909}$

2) Comprova que son inverses l'una de l'altre

$$f : \mathbb{Z}_{4096} \to \mathbb{Z}_{4096} \quad . \quad f(x) = \overline{2957}\,\bar{x}$$
$$g : \mathbb{Z}_{4096} \to \mathbb{Z}_{4096} \quad . \quad g(x) = \overline{3909}\,\bar{x}$$

$mcd(4096, 2957) = 1 \quad \exists \overline{2957}^{-1} \Rightarrow \bar{y} = \overline{2957}\,\bar{x} \Rightarrow \overline{3909}\,\bar{y} = \bar{x} \Rightarrow f^{-1}(\bar{x}) = \overline{3909}\bar{x} = g(\bar{x}).$

332. $n \geq 2 \in \mathbb{Z}$ i p primer
$\sqrt[n]{p}$ irracional.

Demostració : R.A

suposo que $\sqrt[n]{p} \in \mathbb{Q} \Rightarrow \exists a,b \in \mathbb{Z}$ tq $\sqrt[n]{p} = \frac{a}{b}$ $\quad b \neq 0 \quad \wedge \quad mcd(a,b) = 1$,
és a dir $\frac{a}{b}$ fracció irreductible $\Rightarrow p = \frac{a^n}{b^n} \Rightarrow pb^n = a^n \Rightarrow$ Lema d'Euclides
p primer $\wedge$ $p \mid a \cdot a^{n-1} \Rightarrow p \mid a \Rightarrow \exists k \in \mathbb{Z}$ tq $a = pk \wedge a^n = p^n \cdot k^n$ i el mateix
amb b pertant contradicció ja que $mcd(a,b) \neq 1 \Rightarrow p \mid a$ i $p \mid b$.

385. $84x - 133y + a^2 = 1 \quad a \in \mathbb{Z}$

1) Solució $\in \mathbb{Z}$ $(x,y) \Leftrightarrow 7 \mid (1+a) \vee 7 \mid (1-a)$.
$84x - 133y = 1 - a^2$.
$mcd(133, 84) = 7 \Rightarrow 7 \mid 1 - a^2 \Rightarrow 7 \mid (1-a)(1+a) \Rightarrow$ Lema d'Euclides $\Rightarrow 7$ primer
$\Rightarrow 7 \mid (1-a) \vee 7 \mid (1+a)$ cvd.

2) $a = 13$.
$84x - 133y = -168 \Rightarrow mcd(133, 84) = 7 \mid -168 \quad \exists$ solució
Algorisme d'Euclides

1	0	1	−1	2	−5
0	1	−1	2	−3	8
	1	1	1	2	
133	84	49	35	14	7

$\Rightarrow 133(-5) + 84 \cdot 8 = 7 \Rightarrow 84(-192) - 133(-120) = -168$

Solució específica $(x,y) = (-192, -120)$
Solució general

$$\begin{cases} x = -192 - 19t \\ y = -120 - 12t \end{cases} \quad t \in \mathbb{Z}$$

3) x mínima
$x = -192 - 19t \geq 0 \Leftrightarrow t \leq -\frac{192}{19} \simeq -10.1 \Leftrightarrow t \leq -11.$