Universidad Simón Bolívar
Depto. de Matemáticas
Puras y Aplicadas

MA2221 Sept.-dic. 2006
COMPLEMENTOS Y EJERCICIOS
[Claudio Margaglio]

EL ANILLO Z DE LOS ENTEROS

OPERACIONES.
En algunos textos de álgebra se definen los números naturales a partir de la teoría de conjuntos, luego se definen los números enteros (como clases de equivalencia de pares ordenados de naturales) y en el conjunto de los números enteros se definen las operaciones de suma y multiplicación, así como la usual relación de orden. Nosotros supondremos aqui conocer ya el conjunto de los números enteros, con sus operaciones de suma y multiplicación y recordaremos a continuación sus propiedades (estas propiedades las asumiremos en lo que sigue, sin demostrarlas).

Propiedades de la suma (+) y de la multiplicación(*) de enteros.
(**$^+$1**)[Propiedad **asociativa** de la suma],
(**$^+$2**)[Propiedad del **neutro** de la suma],
(**$^+$3**)[Propiedad del **simétrico** de la suma],
(**$^+$4**)[Propiedad **conmutativa** de la suma],
(***1**)[Propiedad **asociativa** de la multiplicación],
(***2**)[Propiedad del **neutro** de la multiplicación],
(***4**)[Propiedad **conmutativa** de la multiplicación],
(**D**)([Propiedad **distributiva** de la multiplicaciónrespecto a la suma].

Con detalle, tenemos :
Suma :
(**$^+$1**) asociativa: $\forall(x, y, z\in \mathbf{Z}) : x+(y+z)=(x+y)+z$;
[**nota** : "$\forall$" significa "para todo"]
(**$^+$2**) del elemento neutro: existe un elemento $0\in \mathbf{Z}$
(que se llamará "cero") tal que: $\forall(x\in \mathbf{Z}) : x+0=0+x = x$;
(**$^+$3**) del elemento simétrico :
Todo elemento $x\in \mathbf{Z}$ tiene "simétrico" ,(que se llamará "opuesto") a saber, un elemento -x tal que $x+(-x) = (-x)+x = 0$.
(**$^+$4**) conmutativa :$\forall(x, y\in \mathbf{Z}) : x+y=y+x$;
Multiplicación :
(***1**) asociativa : $\forall(x, y, z\in \mathbf{Z}) : x*(y*z)=(x*y)*z$;
(***2**) del elemento neutro : existe un elemento,$(\neq 0)$, $1\in \mathbf{Z}$
tal que: $\forall(x\in \mathbf{Z}) : x*1=1*x= x$;
(***4**) conmutativa : $\forall(x, y\in \mathbf{Z}) : x*y=y*x$;
Suma y multiplicación :
D distributiva (de la multiplicación respecto a la suma)
$\forall(x,y,z\in \mathbf{Z}) : x*(y+z)=(x*y)+(x*z)$, $(y+z)*x=(y*x)+(z*x)$.
[Nota : de ahora en adelante definiremos la resta "y-x" así : y-x = y+(-x)].

Indicaremos el conjunto de los números enteros no negativos con $\mathbf{N} = \{0, 1, 2, ...\}$ y como de costumbre lo llamaremos el conjunto de los números naturales;
Indicaremos con $N^*=\{1, 2, ...\}$ el conjunto de los enteros positivos.
Una propiedad del conjunto N de los números naturales, que también supondremos conocida, es la **propiedad del buen orden**
[y esta propiedad es equivalente al principio de inducción]

Propiedad del buen orden : todo subconjunto no vacío de N tiene mínimo

Observación 1: el conjunto de todos los enteros no tiene la propiedad del buen orden; por ejemplo el subconjunto de los enteros negativos no tiene mínimo.
De este punto en adelante, asumiremos como ciertas las propiedades de la suma, multiplicación de los números enteros que hemos considerado así como la propiedad del buenorden para el conjunto de los naturales,
a partir de estas, deduciremos otras.

Ejemplo 1. Demostremos que para cualquier número entero a, se tiene 0.a = 0 .
Tenemos : $0.a \overset{(1)}{=} (0+0).a \overset{(2)}{=} 0.a + 0.a$; luego, si 0.a= b,
podemos escribir : $b = b+b \overset{(3)}{\rightarrow} b+(-b)=(b+b)+(-b) \overset{(4)}{\rightarrow}$
$0 = b+(b+(-b)) \overset{(5)}{\rightarrow} 0 = b+0 \overset{(6)}{\rightarrow} 0 = b$.
Justificación de los pasos de la demostración :
(1), (6) propiedad del neutro de la suma;
(2) propiedad distributiva;
(3), (5) propiedad del simétrico de la suma;
(4) propiedad del simétrico y propiedad asociativa de la suma;

Ejemplo 2.
El opuesto de un número entero siempre es único. Es decir : si b, c son ámbos opuestos de a, entonces debe ser b=c.
Demostración : b = b+0 = b+(a+c) = (b+a)+c = 0+c = c .
Justifique Usted los pasos de esta demostración.

Observación 2. : tomando en cuenta que la suma de enteros es conmutativa y que el opuesto es único, para comprobar que cierto número entero a es opuesto de b, bastará entonces verificar que se tiene a+b = 0 ó b+a = 0 .

Ejemplo 3. Demostremos que :
i) (-a)(b)=-(ab) ,
ii) (-a)(-b)=ab .

i) Gracias a la observación 2, bastará verificar que (-a)(b) es opuesto de ab. En efecto, (-a)(b)+ab = (-a+a)b = 0.b = 0 ;

ii)tomando en cuenta i): (-a)(-b)=-(a(-b))=-(-(ab)); al final, bastará observar que ab , -(-(ab)) son ambos opuestos de -(ab) y por lo tanto, como el opuesto es único, será -(-(ab))= ab.
Nota : Ud. se habrá dado cuenta que también hemos usado (sin mencionarla) la propiedad conmutativa de la multiplicación.

Ejemplo 4. En el anillo , Z, de los números enteros vale la **ley del anulamiento del producto**, es decir : $a\neq 0, b\neq 0, \rightarrow ab\neq 0$.
Tomando en cuenta el ejemplo 3, bastará verificar que si a, b son enteros positivos, entonces ab también es un entero positivo; bastará entonces demostrar la propiedad P(n) = " [para todo entero positivo] $\Rightarrow$ [an= entero positivo] , (siendo $a \geq 1$)

Por lo visto en el ejemplo 4, el anillo de los enteros se llama un **dominio de integridad**

Def. 1. Dominio de integridad.
Un conjunto D con dos operaciones (suma y producto) se llama un **dominio de integridad** si :
i)la suma es asociativa, conmutativa, con neutro , 0, y con la propiedad del simétrico;
[esto se expresa también diciendo que (D, +) es un **grupo conmutativo**]
ii) las multiplicación es asociativa, conmutativa, con neutro , $1 \neq 0$;
[la multiplicación **no** necesariamente tiene la propiedad del simétrico para elementos $\neq 0$]
iii) vale la propiedad distributiva de la multiplicación respecto a la suma;
iv) vale la "ley del anulamiento del producto" es decir, un producto a.b puede ser =0 si y sólo si almenos uno de los dos factores es =0 .

Nota : la propiedad **iv** se expresa a veces diendo que "no hay divisores del cero", ya que si dos elementos no nulos tienen producto =0 se llaman "divisores del cero".

Def. 1'. Cuerpo conmutativo o **campo.**
Un dominio de integridad en el cual valga la propiedad del simétrico para todo elemento $\neq 0$ se llama un "cuerpo conmutativo" o "campo".
Por ejemplo : los conjuntos de **i**) los números racionales , **ii**) los números reales, **iii**) los números complejos,
con las definiciones usuales de suma y multiplicación, son cuerpos conmutativos.
El conjunto $K=\{0, 1\}$, con las operaciones de suma y multiplicación definidas por :
$0+0=1+1=0,\ 0+1=1+0=1,\ 0*0=0*1=1*0=0\ ,\ 1*1=1$
es un cuerpo conmutativo [que denotaremos más adelante con $\mathbf{Z}_2$]

Ejercicio**1.**
Sea E el conjunto de todas las funciones continua $R \to R$, con las usuales operaciones de suma y multiplicación. Verifique que en E (con las operaciones mencionadas) se cumplen las propiedades **i-ii-iii** de la definición de dominio de integridad pero **no** se cumple la **iv**.
[es decir : a) demuestre que se cumplen **i-ii-iii**,
b) proporcione un ejemplo de dos funciones continuas $R \to R$ no nulas, cuyo producto sea la función nula.]
E1.bis Demuestre que en todo dominio de integridad vale la "ley de cancelación" siguiente : $[\ a \neq 0,\ ab=ac\ ] \Rightarrow b=c$

El Principío de inducción .(I_1).
Dada una propiedad P(n) que para todo número natural puede ser cierta o falsa, entonces, si se cumplen las siguientes dos condiciones :

i) $P(n_0)$ es cierta [para cierto número natural, n_0];
ii) $(\forall\ k \in Z,\ k \geq n_0)$: [P(k) cierta] $\to$ [P(k+1) cierta] ;
entonces la propiedad P(n) es cierta para todo $n \geq n_0$.

Proposición 1.
La propiedad del buen orden del conjunto de los números naturales es equivalente al principio de inducción .

Otra forma del Principío de inducción.(II_2).
Dada una propiedad P(n) que para todo número natural puede ser cierta o falsa, entonces, si se cumplen las siguientes dos condiciones :

i) $P(n_0)$ es cierta [para cierto número natural, n_0];
ii) ($\forall$ k$\in$ Z, k $\geq n_0$): [P(n_0), P(n_0+1), P(n_0+2), ...,P(k) cierta]$\rightarrow$ [P(k+1) cierta];
entonces la propiedad P(n) es cierta para todo $n \geq n_0$.

Ud. ya ha visto, en muchas ocasiones, aplicaciones del principio de inducción.

Por supuesto Ud. podrá usar, a su gusto, cualquiera de las varias formas del principio de inducción o, si lo prefiere, la propiedad del buen orden en N.

Ejemplo 5. : definiciones usando inducción.

Def. 2. : potencias con exponente entero no negativo ($a\neq 0$) ,

$$a^n = \begin{cases} 1, \text{ si } n=0 \\ a.a^{n-1}, \text{ si } n>0 \end{cases} ;$$

Def.3. : sumatorias.

$$\sum_{i=0}^{n} a_i = \begin{cases} a_0 \text{ , si } n=0 \\ (\sum_{i=0}^{n-1} a_i)+a_n \text{ , si } n>0 \end{cases} , \quad \sum_{i=m}^{n} a_i = \begin{cases} a_m \text{ , si } n=m \\ (\sum_{i=m}^{n-1} a_i)+a_n \text{ , si } n>m \end{cases} .$$

E2. Demuestre que las siguientes reglas de exponentes :

i) $(a^n)(a^m) = a^{n+m}$; **ii**) $(a^n)^m = a^{nm}$; **iii**)$(ab)^n=a^nb^n$

son válidas para toda escogencia de m, n enteros no negativos

Nota : si a es un elemento no nulo de un cuerpo (por ej. es un número real), se definen potencias con cualquier exponente entero, en la manera siguiente :

$$a^n = \begin{cases} 1, \text{ si } n=0 \\ a.a^{n-1}, \text{ si } n>0 \\ (a^{-1})^{-n} \text{ , si } n<0 \end{cases} .$$

En tal caso, las propiedades mencionadas en el ejercicio **E2** siguen válidas.

E2.bis Demuestre por inducción las siguientes propiedades de las sumatorias :

i) $\sum_{i=0}^{n}(ha_i) = h\sum_{i=0}^{n} a_i$;

ii) $\sum_{i=0}^{n}(a_i+b_i) = \sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i$;

iii) si n<k : $\sum_{i=0}^{k} a_i = \sum_{i=0}^{n} a_i + \sum_{i=n+1}^{k} a_i$;

iv) $\sum_{i=0}^{n} (\sum_{j=0}^{m} a_{ij}) = \sum_{j=0}^{m} (\sum_{i=0}^{n} a_{ij})$.

DIVISIBILIDAD [en un dominio de integridad]

Las siguientes definiciones nos interesan [por el momento] para el caso del anillo de los enteros, pero se pueden dar, en general, para **cualquier dominio de integridad,** por ejemplo en el dominio de integridad de los polinomios en una variable con coeficientes en el cuerpo de los racionales o en el cuerpo de los reales.

Def. 4. Dados a, b$\in$ **D** , se dice que
"b es divisible por a " o que
"a divide b " o que
"b es múltiplo de a " o que
" a es factor de b" o que
" a es divisor de b " ,
si y sólo si existe un elemento c$\in$ **D** tal que b = ca .

E3. Demuestre que la relación definida en D por a $|$b si y sólo si " a divide b" es reflexiva y transitiva.

Def. 5 Dos elementos a, b$\in$ **D** , se dicen asociados si al mismo tiempo a $|$b y b $|$a (es decir : si cada uno es divisor del otro).

Def. 6. Un elemento a$\in$ **D** se dice unitario si y sólo si tiene inverso
(es decir : si y sólo si tiene simétrico respecto a la multiplicación).
En el anillo de los enteros los únicos elementos unitarios son 1, -1 .
¿ cuales son los elementos unitarios en el anillo de los polinomios con coeficientes reales ?

E4. Demuestre que en un dominio de integridad **D** dos elementos no nulos son asociados si y sólo si cada uno de ellos es igual al otro, multiplicado por un conveniente unitario.

E5. Demuestre que en el anillo de los enteros, dos números son asociados si y sólo si tienen el mismo valor absoluto.

E6. Demuestre que la relación de " ser asociados" es una relación de equivalencia en **D** [es decir : es una relación reflexiva, simétrica y transitiva]
Def. 7. factorizaciones **propias** e **impropias.**
Una factorización a=bc de un elemento no nulo ni unitario se dice **propia** si y sólo si ninguno de los dos factores b, c es unitario [y por consiguiente ninguno de los dos factores es asociado con a];
una factorización a=bc se dice **impropia**, si y sólo si uno de los factores es unitario [o equivalentemente, uno de los dos factores es asociado con a].

Por ejemplo en Z : 6=(-2)(-3) es una factorización propia; 6=(-1)(-6) es impropia. $2x^2+4=2(x^2+2)$ es una factorización impropia en el dominio de integridad de los polinomios con coeficientes racionales, Q[x] , mientras que es una factorización propia en Z[x] (polinomios con coeficientes enteros).

Def. 8. elementos **irreducibles** (**primos**)
Un elemento a de un dominio de integridad que no sea ni nulo ni unitario se dice **irreducible** si no tiene ninguna factorización propia, [en el caso de los enteros, esto significa que no tiene ningún divisor diferente de ±1, ± a].
En el caso contrario se dice **compuesto**.
Si el dominio de integridad que se considera es el anillo de los enteros o de los polinomios con coeficientes en un cuerpo, allí "irreducible" es sinónimo de "primo"
Por ejemplo en el anillo de los enteros :
2, 3, 5, 7, -191 son primos ; 4, -6, 200 son compuestos.
Más adelante no enteraremos con mayor detalle del así llamado Teorema fundamental del aritmética que afirma que:
" todo número entero distinto de 0 y de ±1, se puede expresar en forma única, como producto de ±1 por factores primos positivos" [esta factorización es única, a menos del orden en el cual se consideren los factores].

Nota. Def. 8'. elementos **primos.**
En la mayoría de los textos de álgebra, se llama **irreducible** (y no "primo") a un elemento a de un dominio de integridad, **D**, que no sea ni nulo ni unitario y cuyos únicos divisores son elementos unitarios o elementos asociados (recuerde la def. 5).
El nombre de **primo** se le da a elementos, p, que tienen la siguiente propiedad :
* * * * *
si p divide a un producto ab pero no divide el factor a, entonces necesariamente p divide al otro factor, b.
* * * * *
El hecho que en algunos textos de álgebra (por ejemplo nuestro libro de texto así como el texto de G. Birkhoff-S. Mac Lane : "álgebra moderna", editorial Vicens-Vives) se llamen "primos" a los enteros irreducibles, se debe a que se puede demostrar que:
si un entero , n, es irreducible entonces, si n divide a un producto de enteros, ab, pero no divide a uno de los factores, por ejemplo a, entonces necesariamente n divide al otro factor, b.

Ejemplo 6.
El conjunto , **D**, de todos los polinomios con coeficientes reales, cuyo monomio de grado 1 sea nulo, con las definiciones usuales de suma y multiplicación, es un dominio de integridad en el cual "irriducible" no es equivalente a "primo".
$\mathbf{D} = \{ A(x) \in R[x] \mid A(x)= a_0+a_2x^2+...+a_nx^n , a_1=0 \}$.
Por ejemplo se tiene, en **D** : $x^6=x^3x^3=x^2x^4$, x^2 es irreducible pero no es primo, ya que : $x^3 | x^2x^4$ pero no divide a ninguno de los dos factores [tome en cuenta que como $x \notin \mathbf{D}$ no existen las factorizaciones $x^2=x.x$, $x^4= x^3x$ en **D** .

El algoritmo de Euclides en el anillo de los enteros.
Teorema.(**algoritmo de Euclides**)
Dados dos enteros a, b , con b>0 existen (y son únicos) dos enteros q, r [llamados, respectivamente, cociente y resto de la división de a por b] tales que :

i) a=q.b+r ; **ii)** $0 \leq r < b$.

Ejemplo 7. El cociente y el resto de la división de 120 por 17 son : q=7 , r=1 y se tiene 120=7.17+1 ;
el cociente y el resto de la división de -120 por 17 son : q= -8, r=16 y se tiene -120=(-8)17+16 .

Observación 3.(importante)
En el dominio de integridad de los **polinomios** con coeficientes en un cuerpo [por ej. coeficientes reales] también vale el siguiente algoritmo de división :

Dados dos polinomios A(x), B(x) , con $B(x) \neq 0$ existen (y son únicos) dos polinomios q(x), r(x) [llamados, respectivamente, cociente y resto de la división de A(x) por B(x)] tales que :

i) A(x)=B(x)q(x)+r(x) **ii)** grado(r(x))< grado (B(x))

[con el convenio que el poliomio nulo tenga grado =-1 y todo polinomio constante no nulo tenga grado =0]

Def. 9 : máximo común divisor.
Un número entero positivo $d \in N^*$ se llama máximo común divisor de los números enteros a, b y se indica con el símbolo **(a, b)** , si se cumplen las siguientes condiciones:
i) $d \mid a$, $d \mid b$ (es decir d es divisor de ambos, a, b);
ii) d es el máximo de todos los divisores comunes de a, b.

Observación 4 [importante].
la condición ii) se reemplaza a veces con la siguiente :
ii*) si d ' es cualquier divisor común de a, b entonces $d' \mid d$.

Esta segunda condición parece menos sencilla que la ii) sin embargo es muy importante ya que **a**) en el caso de considerar el concepto de máximo común divisor en el conjunto de los naturales es equivalente a ii);
b) tiene sentido en cualquier dominio de integridad, por ejemplo en el dominio de integridad de los polinomios con coeficientes en un cuerpo
[por ej. coeficientes reales];
Usando para la definición de máximo común divisor las dos condiciones i), ii*) en el conjunto N , de los Naturales se obtiene lo mismo que la definición 9;
Para obtener lo mismo que con la def. 9 en el dominio de integridad Z, de los enteros, habría que agregar la condición que el máximo común divisor sea positivo, ya que de otra manera, por ejemplo, un máximo común divisor de 4, 6 podría ser 2 y también -2;
En el dominio de integridad R[x], de los polinomios con coeficientes reales, la condición ii) no tiene sentido mientras que la ii*) sí; también en este caso se presenta el inconveniente de que el máximo común divisor no sería único, ya que por ejemplo cualquier polinomio del tipo ax^2+a sería máximo común divisor de los dos polinomios x^4+2x^2+1, x^4+x^2-2 ; sin embargo, agregando la condición de que el máximo común divisor sea un polinomio "mónico" [es decir con el coeficiente del monomio de grado máximo =1] se lograría la unicidad del máximo común divisor.
[**aqui termina la observación importante**]

E7. demuestre que en un dominio de integridad, D, dados dos elementos no nulos a, b, si c cumple con la definición de "máximo común divisor de a, b" con las condiciones i), ii*), entonces :

a) si k es unitario [ver def. 6] entonces c ' = k.c también cumple con las mismas condiciones;
b) si c ', c" son dos elementos que cumplen ámbos con las condiciones i), ii*) entonces necesariamente c', c" son asociados, es decir uno es igual al otro multiplicado por un unitario.

E8. Considere la formación del máximo común divisor como una operación en el conjunto de los enteros positivos, N*.
Es decir, m*n=M.C.D(m,n) = (m,n) ;
por ejemplo 15*18=3 , 200*48=8 etc.
Averigue si esta operación tiene las propiedades :
a) conmutativa ; b) asociativa ; c) del neutro.

Usando el algoritmo de la división de Euclides, se puede demostrar el siguiente:

Teorema 2.
El máximo común divisor, (m,n), de dos enteros, m, n, no nulos, cualesquiera, siempre se puede expresar como combinación lineal (con coeficientes enteros) de los números dados : d = sm+tn.

Observación 5.
Como la demostración del teorema 2 se logra gracias al algoritmo de la división euclídea, lo mismo puede hacerse en el dominio de integridad de los polinomios con coeficientes en un cuerpo.

Ejemplo 8.
Sea m= 4697 , n= 1331 ; su máximo común divisor es 11 y se tiene, por ejemplo :
11 = (-17).4697+60.1331.
¿ Como se pudo saber que con s=-17 y t=60, la combinación lineal sm+tn daba como resultado justamente el máximo común divisor, 11 de m, n ? Dentro de un momento nos enteraremos como se puede proceder.

Ejemplo 9.
Sean $A(x) = x^3+3x-4$, $B(x)= x^3+x^2-2$; se tiene (A, B)= x-1 y una combinación lineal (con coeficientes polinomiales) cuyo valor es el máximo común divisor de A, B es : $(\frac{x}{10} + \frac{2}{5})\, A(x) + (\frac{-x}{10} - \frac{3}{10})B(x) = x-1$.

Demostración del teorema 2.
Observemos ante todo, que no es restrictivo suponer que m, n sean enteros positivos. En efecto, si uno de los dos números (o ambos) cambia de signo, el máximo común divisor queda el mismo, (ya que todo entero es asociado de su opuesto), y en cuanto a los coeficientes de la combinación lineal, bastaría cambiar de signo el correspondiente coeficiente (s y/o t);
por ejemplo, si en el ejemplo 8 se hubiesen considerado los dos números -4697, 1331, el M.C.D seguiría siendo 11 y la combinación lineal habría cambiado en :

11 = 17.(-4697)+60.1331.

Por lo tanto haremos nuestra demostración suponiendo que m, n sean enteros positivos.

Indicaremos m, n con los símbolos $m=r_1$, $n=r_2$, y el resto de la división de m por n, con r_3 : $r_1 = q_1.r_2 + r_3$, luego seguiremos dividiendo sucesivamente : $r_2 = q_2.r_3 + r_4$, $r_3 = q_3.r_4 + r_5$,...
hasta que por primera vez, cierto resto r_k sea nulo.
esto se cumplirá seguramente, ya que, como sabemos, en toda división euclídea, el resto siempre es no negativo y estrictamente menor que el divisor; por lo tanto, en la primera división será : $0 \leq r_3 < r_2$, en la segunda $0 \leq r_4 < r_3$, y por lo tanto : $0 \leq ... r_i < r_{i-1} < ... r_3 < r_2 = n$. Como el resto en cada división es estrictamente menor que el resto de la división anterior, llega necesariamente el momento en que cierto resto es nulo.
Verificaremos entonces que :

1) el último resto no nulo es el M.C.D(m, n) ;
2) usando las divisiones que se han efectuado, es posible (en varias maneras) hallar los coeficientes s, t que proporcionan la combinación lineal $d = sm+tn$.

Ejemplo 10.
Con referencia a los números del ejemplo 8, tenemos :
(1) : $4697=3.1331+704$; $r_1=4697$, $r_2=1331$, $r_3=704$, $q_1=3$;
(2) : $1331=704+627$; $r_4=627$, $q_2=1$;
(3) : $704=627+77$; $r_5=77$, $q_3=1$;
(4) : $627=8.77+11$; $r_6=11$, $q_4=8$;
(5) : $77=7.11+0$; $r_7=0$, $q_5=7$;
el último resto no nulo es : $r_6=11$ que es (como demostraremos) el M.C.D. (4697, 1331) ;

Una primera alternativa para obtener el M.C.D. como combinación lineal de los números dados, m, n, es la siguiente :
expresar el M.C.D. como combinación lineal de los restos anteriores, por medio de la penúltima división (4):
$r_6=11= 627- 8.77 = r_4- 8.r_5$, luego usar la división anterior (3) para expresar r_5 por medio de r_3, r_4 y así siguiendo, obtener al final una combinación lineal en la cual aparecen sólo r_1, r_2 es decir, m, n .
Obtenemos sucesivamente : $11 \overset{(4)}{=} 627- 8.77 \overset{(3)}{=}$
$= 627- 8.(704-627) = 9.(627)+(-8).704 \overset{(2)}{=}$
$=9.(1331- 704)+(-8).704 = 9.1331+(-17).704 \overset{(1)}{=}$
$=9.1331+(-17)(4697-3.1331) = 60.1331+(-17).4697$.

Es decir, hemos obtenido la combinación lineal que buscábamos : $11 = 60.1331+(-17).4697$.

Una segunda alternativa (que resulta mejor si se quiere efectuar el proceso por medio de un programa de computadora) es la siguiente :
Construyamos dos sucesiones de números ,
$x_1, x_2, ...$, $y_1, y_2, ...$, en la manera siguiente :
$x_1=1$, $x_2=0$, $y_1=0$, $y_2= 1$ y a partir del subíndice 3, contruyamos
x_i por medio de x_{i-1} , x_{i-2} con la misma fórmula con la cual se genera r_i por medio de r_{i-1} , r_{i-2} y lo mismo con y_i por medio de y_{i-1} , y_{i-2} a título de ejemplo, teníamos

$r_1 = q_1.r_2 + r_3$ es decir : $r_3 = r_1 - q_1.r_2$ luego pondremos
$x_3 = x_1 - q_1.x_2$ y lo mismo haremos con la sucesión de las y_i :
$y_3 = y_1 - q_1.y_2$; en general, para un genérico subíndice k será :
$x_k = x_{k-2} - q_{k-2}.x_{k-1}$, $y_k = y_{k-2} - q_{k-2}.y_{k-1}$.

Se puede demostrar entonces por inducción (2a forma), I_2, que para todo subíndice k, se tiene : $x_k.m + y_k.n = r_k$ y por lo tanto, con aquel subíndice "k" que corresponde al último resto no nulo, se obtiene la combinación lineal buscada.

E9. Demuestre por inducción (I_2) que construyendo en la manera indicada las sucesiones $x_1, x_2, \ldots$, $y_1, y_2, \ldots$, se obtiene para todo subíndice k (mientras los restos de las divisiones no sean nulos): $x_k.m + y_k.n = r_k$.

[Sugerencia : verifique la fórmula para k=1, k=2 y luego, admitiéndola cierta para i=k-1 , i=k , demuéstrela para k+1.
Sigue la **demostración del teorema 2**.
(1) $r_1 = q_1.r_2 + r_3$;
(2) $r_2 = q_2.r_3 + r_4$;
(3) $r_3 = q_3.r_4 + r_5$;
.....
(k-2) $r_{k-2} = q_{k-2}.r_{k-1} + r_k$;
(k-1) $r_{k-1} = q_{k-1}.r_k + 0$.
[es decir: supongamos que el último resto no nulo sea r_k].
Por ser r_k un resto no nulo, será evidentemente un entero positivo; tendremos que verificar que cumple con las dos condiciones pedidas en la definición 8.
1) ¿ Divide r_k a los dos números $m=r_1$, $n=r_2$?

E10. Sean a, b, c, s, t elementos de cierto dominio de integridad, **D**;
Demuestre que si c divide a y divide b entonces c también divide s.a+t.b.

Vemos que r_k divide a r_{k-1} (fórmula de la última división);
como r_{k-2} es combinación lineal de r_k , r_{k-1}
(fórmula de la penúltima división: (k-2)), por el resultado del ejercicio E10,
r_k dividirá r_{k-2} (además de dividir r_{k-1}) ;
luego , considerando la fórmula de la división anterior (k-3), podemos constatar que r_k debe dividir r_{k-3} (además de r_{k-2});
así siguiendo se llega al final a constatar que r_k debe dividir a r_1, r_2 es decir m, n .
2) Si d' divide a m, n , dividirá d ?
Esta vez pasaremos en revista las varias fórmulas de las divisiones, en el sentido desde la primera hacia la última :
de la primera : (1) $r_1 = q_1.r_2 + r_3$;
resulta que como $r_3 = r_1 - q_1.r_2$ es combinación lineal de r_1, r_2
(es decir, de m, n) , por el resultado del ejercicio E10, d' dividirá
a r_3 ; luego de la segunda , resulta que $r_4 = r_2 - q_1.r_3$ es combinación lineal de r_2, r_3
luego, de nuevo por el ejercicio E10, d' dividirá r_4; así siguiendo, se demuestra que d' debe dividir a r_4, r_5, ... , $r_k = d$.

Aqui termina la demostración del hecho que el último resto no nulo en el procedimiento que estamos estudiando, es el M.C.D. de los dos números m, n considerados.

E11. Halle el M.C.D. de los siguientes pares de números, y expréselo como combinación lineal de los mismos :
a) 25, 105 ; **b**) 48 , 300 ; **c**) 1331, 671 ; **d**) 1000, 121 .

E12. Halle el M.C.D. de las siguientes ternas de números, y expréselo como combinación lineal de los mismos:
a) 6, 10, 15 ; **b**) 2662 , 484 , 3993 .

E13. Averigue como se podría aplicar el procedimiento del teorema 2, para hallar el M.C.D. de un número n>3 de números enteros;
(por ejemplo M.C.D.(30, 42, 70, 105)).

E14. Sean a_1, a_2, a_3, b, c enteros no nulos y sea $c= a_1+a_2+a_3 \neq 0$;
demuestre que si b divide a : c , a_1, a_2, entonces b necesariamente debe dividir también a a_3 .

Aplicación 1 : el derecho de llamar "primos" a los enteros irreducibles.
[en los dominios de integridad de los enteros y de los polinomios con coeficientes en un cuerpo]
Demostremos (usando el teorema 2) que si un número entero irrreducible, c, divide a un producto ab entonces necesariamente c divide a uno de los factores.
Verificaremos que si c divide al producto ab pero no divide al factor a, entonces c divide necesariamente al otro factor, b.
Veamos cual puede ser el máximo común divisor de a,c :
como debe ser un divisor de c y por hipótesis c es irreducible (luego c es divisible sólo por unitarios o asociados) los únicos "candidatos" a M.C.D.(a, c) son : 1 y c (o -c, si c es negativo) y como por hipótesis c no divide a a, la única posibilidad que queda es M.C.D.(a, c) = 1 .
Entonces por el teorema 2 podemos escribir : 1 =sa+tc , con convenientes enteros s, t y también, multiplicando por b :
b = bsa+btc = s(ab)+(bt)c ; resulta así que b es suma de dos sumandos, ambos múltiplos de c [ya que por hipótesis, c divide ab] y por lo tanto (recuerde el ejercicio E10) c divide a b].
Aplicación 2.(generalización de la aplicación 1).
Dados cuatro enteros a, b, c, d , si cd=ab y si M.C.D.(a, c)=1
(es decir si a, c no tienen factores comunes, a no ser ±1) ,
entonces necesariamente c divide a b y a divide a d.
[La demostración es igual a la de la aplicación 1].
Ejemplo 11. Si a, b son dos enteros no nulos y el producto ab es divisible por 18 pero a no es divisible ni por 2 ni por 3, entonces b tiene que ser multiplo de 18.
Por ejemplo si se tiene 18d=85b (con b, d enteros no nulos)
entonces b es necesariamente múltiplo de 18
[¡ y d es múltiplo de 85 ! ; explique...].
E15. Demuestre que si p es primo y si p divide a un producto de tres enteros no nulos a.b.c , entonces p divide a almenos uno de los tres a, b, c.

E16. Demuestre por inducción, la propiedad P(n) : si un primo p divide a un producto $a_1a_2...a_n$ de n enteros no nulos, entonces necesariamente p divide a almenos uno de los factores a_i .

Ejemplo 12. (**importante**)Recuerdo de un método que se usa a veces en Bachillerato para hallar soluciones racionales para ecuaciones polinómicas con coeficientes enteros.

Si $f(x) = a_nx^n+a_{n-1}x^{n-1}+...+a_2x^2+a_1x+a_0$ es un polinomio con coeficientes enteros y si $\frac{p}{q}$ es una fracción de enteros irreducible [es decir : M.C.D.(p, q) = 1] tal que $f(\frac{p}{q}) = 0$, entonces necesariamente p divide a_0 y q divide a_n .

Por ejemplo, aplicando este criterio, nos podemos enterar que las posibles soluciones racionales de la ecuación $x^3+3x+2=0$ deberían ser una de las siguientes : ±1 , ±2 , ya que por ser el coeficiente $a_n=a_3=1$, el denominador q debe ser ±1 y por ser $a_0= 2$, el numerador debe ser ±1 o ±2. Como ninguno de los cuatro números que así se obtienen, [±1 , ±2], anula al polinomio x^3+3x+2, podemos concluir que la ecuación dada no tiene soluciones racionales .

E17. Conociendo que la ecuación $4x^4-3x^2-7x-3 = 0$
tiene almenos una solución racional, halle todas las soluciones de la ecuación.
[Sugerencia: aplique el método del ejemplo 12].

E18. Diga con cuales fracciones (y/o enteros) hay que calcular el valor del polinomio $6x^3+x-4$ para hallar sus posibles ceros racionales o para asegurar que no tiene.
[habría que hacer 16 averiguaciones...]

E19. Demuestre la validez del método enunciado en el ejemplo 12, usando la aplicación 2.

El teorema fundamental del aritmética.

" todo número entero distinto de 0 y de ±1, se puede expresar en forma única, como producto de ±1 por factores primos positivos" [esta factorización es única, a menos del orden en el cual se consideren los factores].

Demostraremos este teorema en dos partes :
1) existencia de la factorización,usando el principio de inducción;
2) unicidad de la factorización (a menos del orden de los factores), usando inducción y la aplicación 1 del teorema 2.

1 : Demostración de la existencia de la factorización, para todo entero distinto de 0 y ±1 : no es restrictivo suponer que el número entero que consideramos sea positivo, ya que si m es negativo y si su opuesto tiene la factorización -m=a.b.c , entonces podemos escribir m = (-1).a.b.c .
Si n es positivo ≥ 2, consideremos la propiedad:
P(n) : "n se puede obtener como producto del número 1 por cierto número de factores enteros irreducibles (primos) positivos";
Como P(2) es cierta, ya que 2=1.2 y 2 es primo, bastará que cumplamos con la segunda parte de la demostración, usando el principio de inducción en la forma $\mathbf{I_2}$.
Supongamos cierta P(i) para todo natural i= 2, 3,...,k y tratemos de demostrar P(k+1); observemos que si el número k+1 es primo, entonces P(k+1) es cierta, ya

que podemos escribir k+1=1.(k+1), (así como lo hicimos con el número 2); si por otra parte k+1 no es primo, será posible factorizarlo : k+1=a.b de manera que ninguno de los dos factores a, b sea unitario o asociado a k+1. Esto implica que ambos factores a, b son números enteros positivos estríctamente menores que k+1, por lo cual P(a), P(b) son ciertas (por hipótesis inductiva), de manera que se factorizan cada uno en producto : $a=1.p_1p_2...p_r$, $b=1.q_1q_2...q_s$, con $p_1,p_2...p_r,q_1,q_2...q_s$, primos positivos, y entonces podemos escribir también: $k+1=ab=(1.p_1p_2...p_r)(1.q_1q_2...q_s)=1.p_1p_2...p_rq_1q_2...q_s$ como producto de primos positivos.

2: Demostración de la unicidad de la factorización;
Demostraremos, por inducción, la siguiente propiedad
P(n) : si un entero positivo tiene dos factorizaciones :
$a = 1.p_1p_2...p_r = 1.q_1q_2...q_n$ con $1 \le r \le n$, entonces necesariamente r=n y los factores $.p_1, p_2,.., p_r$ son los mismos que los factores $q_1, q_2,..., q_n$ (talvez en otro orden).
Averiguemos que P(1) es cierta:
si $n = 1$, $1 \le r \le n=1$ entonces r=n=1 y $a=1.p_1= 1.q_1$; evidentemente debe ser $p_1= q_1$;
Supongamos ahora que P(k) sea cierta y consideremos dos factorizaciones de cierto número entero positivo como las siguientes : $a = 1.p_1p_2...p_r = 1.q_1q_2...q_{k+1}$;
como el primo q_{k+1} divide al producto $1.p_1p_2...p_r$, por el resultado del ejercicio E16, debe dividir a almenos uno de los factores p_i y, cambiando eventualmente el orden de los p_i , no es restrictivo suponer que divida justamente a p_r ; pero como p_r también es primo y sus únicos divisores son ±1 y $\pm p_r$ la única posibilidad que hay, es que sea $q_{k+1}= p_r$, podemos entonces simplificar, y escribir : $p_1p_2...p_{r-1} = 1.q_1q_2...q_k$ y ahora, por hipótesis inductiva (como suponemos cierta P(k)), los factores $p_1, p_2, ...p_{r-1}$ son los mismos que los $q_1, q_2,..., q_k$.
[Nota : hemos podido usar la hipótesis inductiva, ya que por ser $r \le k+1$, tenemos también $r-1 \le k$] .
Aqui termina la demostración del teorema fundamental del aritmética.

<u>Observación 6</u> (importante).
Ahora que sabemos que todo entero distinto de 0 y ±1 se factoriza en manera única en producto de ±1 por cierto número de factores primos positivos, podemos enterarnos que una forma alterna de hallar el M.C.D. de dos enteros no nulos a, b es la que hemos aprendido en Bachillerato :
Dados dos enteros a, b distintos de 0 y ±1 , su M.C.D. se puede obtener como producto de todos sus factores primos comunes, con el mínimo exponente.
Por ejemplo, M.C.D.(252, 600)= 12 ; por otra parte $252=2^2.3^2.7$;
$600 = 2^3.3.5^2$; los factores comunes son 2, 3 y los exponentes mínimos son : 2, para el primo 2 , 1 para el primo 3 , de manera que M.C.D.(252, 600)= $2^2.3= 12$.

E20. Trate de <u>demostrar</u> lo que se afirmó en la observación 6.

Def. 10. : mínimo común múltiplo.
Dados dos enteros no nulos, a, b, se define su mínimo común múltiplo

m = m.c.m.{a, b} = [a, b] como aquel único entero positivo , m , que tenga las siguientes propiedades:
i) a $\mid$m , b $\mid$m (es decir : m es múltiplo de a, b);
ii) si a $\mid$m' , b $\mid$m' , entonces necesariamente m $\mid$m' .
Nota. Igual que en el caso del máximo común divisor, si se quiere que el mínimo común múltiplo, m, sea único hay que exigir : en el caso de los enteros, que sea m > 0 y en el caso de los polinomios que m sea polinomio mónico.

Otra aplicación del algoritmo de Euclides :
Existencia del mínimo común múltiplo.
Sean a, b enteros no nulos y sea E={x∈ **Z** $\mid$ x es múltiplo de a, b};
observemos que E≠Ø ya que por ejemplo a.b∈ E y también observemos que seguramente E contiene números enteros positivos, ya que si por ejemplo a.b fuese negativo, su opuesto, -a.b es positivo y también pertenece a E.
Por el principio del buen orden el subconjunto
H=E∩N* (≠Ø) , formado por todos los enteros positivos que son múltiplos comunes de a, b, tiene mínimo, m .
Si x∈ E , y si dividimos x por m, con el algoritmo de la división de Euclides :
x=q.m+r , tenemos que r = x - q.mx ∈ E (ya que por ser ambos, x , q.m , múltiplos de m, su resta también será múltiplo de m);
como 0 ≤ r< m (= divisor en la división) y m era el menor entero positivo entre los múltiplos comunes de a, b, necesariamente r debe ser =0 ; pero entonces la división de x por m es exacta y tenemos que x es múltiplo de m, es decir m divide a x.
Por lo tanto el número m que estamos considerando, además de ser múltiplo común de a, b, divide a todo múltiplo común de a, b , es decir, cumple con la definición de m.c.m.(a, b) .

E21. Demuestre que el M.C.D., (a, b) es único.

E22. Demuestre que el m.c.m. de dos enteros no nulos, factorizados en producto de primos, se puede obtener como el producto de los factores comunes y no comunes, cada uno con el máximo exponente.
Por ejemplo m= m.c.m.(252, 600)= 12600 ; por otra parte
$252=2^2.3^2.7$; $600 = 2^3.3.5^2$; $m = 2^3.3^2.5^2.7 = 12600$;
a.b = (252).(600)=151200 = (12).(12600) = d.m .

E23. Demuestre que si d= (m, n)=M.C.D.{m, n} , k= [m, n]=m.c.m.{m, n}
entonces : **i**) si m, n son enteros positivos entonces : d.k = m.n ;
ii) si m, n son enteros cualesquiera entonces d.k = $\mid$m.n$\mid$;
iii) si m, n son polinomios o enteros, entonces d.k =u. m.n, siendo u=unitario
E24. Demuestre que hay infinitos números primos.
[Sugerencia : si los números primos fuesen solamente
$p_1, p_2, ...p_n$ entonces considere el número a= $p_1p_2...p_n$ +1;
si a es primo, es diferente de $p_1, p_2, ...p_n$; si a no es primo, por el teorema fundamental del aritmética, será producto de primos, ninguno de los cuales podrá ser uno de los $p_1, p_2, ...p_n$];

a título de ejemplo, si los primos fuesen solamente 2, 3, 5, 7, podríamos considerar 2.3.5.7+1 = 211 que, por no ser múltiplo ni de 2 ni 3 ni 5 ni 7 deberá tener factores primos diferentes].

E25. Diga, justificando si se puede o no expresar el número 81 como combinación lineal 81 = s.a+t.b (con coeficientes enteros s, t), siendo a=3000 , b=8751 ; en caso afirmativo, halle números enteros s, t de manera que s.3000+t.8751 = 81.

E26. Diga justificando :
a)si los enteros s, t tales que s.3000+t.8751 = 81 , son únicos;
b) diga si es posible hallar s, t enteros, de manera que s sea negativo.

E27. Para cada una de las siguientes afirmaciones, diga, justificando, si es cierta o falsa :
a) la operación, definida en **Z*** (conjunto de los enteros no nulos) por n*m=m.c.m.(n, m) es asociativa;
b) M.C.D.(a.m, a.n)= a.M.C.D.(m, n) ;
c) si d= M.C.D.(m, n) y si $h=\frac{m}{d}$, $k=\frac{n}{d}$, entonces M.C.D.(h, k)=1.

E28. Demuestre la parte de la "existencia" del teorema fundamental del aritmética, usando el principio del buen orden en lugar del principio de inducción.
[Sugerencia : suponga que exista un número entero (>1) que no se puede expresar como producto de primos positivos, entonces será $\neq\varnothing$ el subconjunto , E, de **N*** , formado por los enteros positivos (mayores que 1) que no se pueden expresar como producto de primos positivos ; tal conjunto E, por la propiedad del buen orden, tendrá mínimo, m ; este mínimo no será primo (ya que en tal caso sería producto de primos, con un solo factor, ...etc.].

E29. Demuestre directamente (adaptando la demostración general a este caso particular) que no es posible que cierto entero positivo n tenga dos factorizaciones como las siguientes :
$n= p_1p_2= q_1q_2q_3$, siendo p_1, p_2, q_1, q_2, q_3 primos.

E30. Sean a un número entero par y b un entero impar.
i)Demuestre que entonces (a+b, a-b) = (a, b) ;
ii) proporcione ejemplos de pares de enteros. ámbos pares o ámbos impares tales que (a+b, a-b) ≠ (a, b) ;
iii) averigue si es posible que sea (a+b, a-b) = (a, b) en el caso que a, b tengan la misma paridad.

Soluciones de los ejercicios desde E1 hasta E30.

SE1.- La verificación de las propiedades de suma y multiplicación (así como la propiedad distributiva) en en conjunto de las funciones continuas R→R se logra tomando en cuenta :
a) la definiciones de suma y multiplicación de funciones :
(f+g)(x)=f(x)+g(x), (f*g)(x)=f(x)g(x) ;
b) las propiedades correspondientes de suma y multiplicación de números reales.

Por ejemplo, verifiquemos la D (distributiva) :

$(f*(g+h))(x) \underset{(1)}{=} f(x)(g+h)(x) \underset{(2)}{=} f(x)(g(x)+h(x)) \underset{(3)}{=}$

$\underset{(3)}{=} f(x)g(x)+f(x)h(x) \underset{(4)}{=} (f*g)(x)+(f*h)(x) \underset{(5)}{=} ((f*g)+(f*h))(x)$.

Justificación : definición de producto de funciones : (1), (4) ;
definición de suma de funciones : (2), (5) ;
propiedad distributiva en **R** : (3) .
Un ejemplo de dos funciones continuas no nulas, cuyo producto es la función nula, puede ser el siguiente : $f(x)=|x|+x$, $g(x)=|x|-x$.

SE1.bis. $a\neq 0$, $ab=ac \Rightarrow ab-ac = a(b-c)= 0 \Rightarrow$ [uno de los dos factores debe ser nulo y como $a\neq 0$ será $b-c=0$ por lo cual $b=c$].

SE2.
i) Sea **P(n) =** "$(a^n)(a^m) = a^{n+m}$ es cierta para todo entero no negativo, m " ;
Usando el principio de inducción en su primera forma
$P(0) : (a^0)(a^m) = 1.a^m = a^m = a^{0+m}$ cierto [def. 2] ;
$P(k+1) : (a^{k+1})(a^m) \underset{(1)}{=} (a.a^k)(a^m) \underset{(2)}{=} a(a^k a^m) \underset{(3)}{=} a(a^{k+m}) \underset{(4)}{=} a^{k+m+1}=a^{(k+1)+m}$;

justificación : (1), (4) : def. 2 ;
(2) : propiedad asociativa de la multiplicación;
(3) : hipótesis inductiva .

ii) Sea **Q(m) =** "$(a^n)^m = a^{nm}$ "es cierta para todo entero no negativo, n" ;
$Q(0) : (a^n)^0 = 1 = a^0 = a^{n0}$;
$Q(k+1) : (a^n)^{k+1} \underset{(1)}{=} (a^n)(a^n)^k \underset{(2)}{=} (a^n)((a^{nk}) \underset{(3)}{=} a^{n+nk}= a^{n(k+1)}$;

justificación : (1) : def. 2 ; (2) : hipótesis inductiva ; (3) : propiedad **i**) de este ejercicio;

iii) Sea **S(n) =** " $(ab)^n=a^n b^n$ para todo entero n, no negativo ";
$S(0) : (ab)^0= 1 = 1.1 = a^0 b^0$;
$S(k+1) : (ab)^{k+1} \underset{(1)}{=} (ab)(ab)^k \underset{(2)}{=} (ab)(a^k b^k) \underset{(3)}{=} (a.a^k)(b.b^k) \underset{(4)}{=} a^{k+1}b^{k+1}$;

justificación : (1), (4) : def. 2 ; (2) : hipótesis inductiva ;
(3) : propiedades asociativa y conmutativa de la multiplicación.

SE2.bis.
i) $P(n) : \sum_{i=0}^{n}(ha_i) = h\sum_{i=0}^{n}a_i$;
$P(0) : \sum_{i=0}^{0}(ha_i) = ha_0 = h\sum_{i=0}^{0}a_i$;

$P(k+1): \sum_{i=0}^{k+1}(ha_i) \underset{(1)}{=} \sum_{i=0}^{k}(ha_i) + ha_{k+1} \underset{(2)}{=} h\sum_{i=0}^{k}a_i + ha_{k+1} \underset{(3)}{=} h(\sum_{i=0}^{k}a_i + a_{k+1}) \underset{(4)}{=} h\sum_{i=0}^{k+1}a_i$

justificación : (1), (4) : def. 3 ; (2) hipótesis inductiva ; (3) propiedad distributiva.

ii) $P(n): \sum_{i=0}^{n}(a_i+b_i) = \sum_{i=0}^{n}a_i + \sum_{i=0}^{n}b_i$;

$P(0): \sum_{i=0}^{0}(a_i+b_i) = a_0+b_0 = \sum_{i=0}^{0}a_i + \sum_{i=0}^{0}b_i$ [def. 3] ;

$P(k+1): \sum_{i=0}^{k+1}(a_i+b_i) \underset{(1)}{=} (\sum_{i=0}^{k}(a_i+b_i))+(a_{k+1}+b_{k+1}) \underset{(2)}{=} (\sum_{i=0}^{k}a_i+\sum_{i=0}^{k}b_i)(a_{k+1}+b_{k+1}) \underset{(3)}{=}$

$\underset{(3)}{=}(\sum_{i=0}^{k}a_i)+a_{k+1}+(\sum_{i=0}^{k}b_i)+b_{k+1} \underset{(4)}{=} \sum_{i=0}^{k+1}a_i + \sum_{i=0}^{k+1}b_i$;

justificación : (1), (4) : def. 3 ; (2) hipótesis inductiva ;
(3) propiedad asociativa y conmutativa de la suma;

iii) $P(s)$: si $n<s$: $\sum_{i=0}^{s}a_i = \sum_{i=0}^{n}a_i + \sum_{i=n+1}^{s}a_i$;

$P(1)$: si $s=1$, necesariamente será $n=0$, luego : $\sum_{i=0}^{0}a_i + \sum_{i=0+1}^{1}a_i = a_0+a_1 = \sum_{i=0}^{1}a_i$;

$P(k+1)$: si $n=k$ entonces $\sum_{i=0}^{k+1}a_i \underset{(1)}{=} (\sum_{i=0}^{k}a_i)+a_{k+1} \underset{(2)}{=} (\sum_{i=0}^{k}a_i)+ (\sum_{i=k+1}^{k+1}a_i)$; si $n < k$ entonces :

$\sum_{i=0}^{k+1}a_i \underset{(3)}{=} (\sum_{i=0}^{k}a_i)+a_{k+1} \underset{(4)}{=} ((\sum_{i=0}^{n}a_i)+(\sum_{i=n+1}^{k}a_i))+a_{k+1} \underset{(5)}{=} (\sum_{i=0}^{n}a_i)+((\sum_{i=n+1}^{k}a_i)+a_{k+1}) \underset{(6)}{=}$

$= (\sum_{i=0}^{n}a_i)+\sum_{i=n+1}^{k+1}a_i$

justificación : (1), (2), (3). (6) : def. 3 ; (4) hipótesis inductiva ;
(5) propiedad asociativa de la suma;

iv) $P(n)$: " $\sum_{i=0}^{n}(\sum_{j=0}^{m}a_{ij}) = \sum_{j=0}^{m}(\sum_{i=0}^{n}a_{ij})$ para todo entero no negativo, m " ;

$P(0): \sum_{i=0}^{0}(\sum_{j=0}^{m}a_{ij}) = \sum_{j=0}^{m}a_{0j} = \sum_{j=0}^{m}(\sum_{i=0}^{0}a_{0j})$;

$P(k+1): \sum_{i=0}^{k+1}(\sum_{j=0}^{m}a_{ij}) \underset{(1)}{=} \sum_{i=0}^{k}(\sum_{j=0}^{m}a_{ij}) + (\sum_{j=0}^{m}a_{k+1,j}) \underset{(2)}{=} \sum_{j=0}^{m}(\sum_{i=0}^{k}a_{ij}) + (\sum_{j=0}^{m}a_{k+1,j}) \underset{(3)}{=}$

$= \sum_{j=0}^{m}((\sum_{i=0}^{k}a_{ij})+a_{k+1,j}) \underset{(4)}{=} \sum_{j=0}^{m}(\sum_{i=0}^{k+1}a_{ij})$;

justificación : (1), (4) : def. 3 ; (2) hipótesis inductiva ;
(3) propiedad **ii**) de este ejercicio.

SE3. $a=1.a \Rightarrow a|a$ por lo cual la relación "|" es reflexiva;
$a|b, b|c \Rightarrow b=c_1a, c=c_2b \Rightarrow c=(c_2c_1)a \Rightarrow a|c$ por lo cual "|" es transitiva.

SE4. Si a , b son asociados, entonces $a|b$, $b|a$ luego existen elementos $c_1, c_2 \in \mathbf{D}$ tales que $b=c_1a$, $a=c_2b$ luego $a=(c_2c_1)a \Rightarrow (c_2c_1)=1 \Rightarrow c_1, c_2$ son unitarios.

SE5. Por el ejercicio anterior, si a, b son asociados entonces $b=c_1a$, con c_1 unitario; y como los únicos unitarios en **Z** son ±1 sigue que $|a|=|b|$.

SE6. i**)**como a=1.a , todo elemento, a, es asociado consigo mismo por lo cual la relación es **reflexiva**;
ii) si b es asociado con a entonces $b=c_1a$, con c_1 unitario [E4] , luego $a= (c_1)^{-1}b$, es decir, a es asociado con b ; por lo tanto la relación es **simétrica**;
iii) si b es asociado con a, c es asociado con b, entonces existen elementos unitarios c_1, c_2 , tales que $b=c_1a$, $c=c_2b$ por lo cual $c=(c_2c_1)a$.
[observe que el producto de dos unitarios es unitario, ya que $((c_1)^{-1}(c_2)^{-1})(c_2c_1) = (c_1)^{-1}((c_2)^{-1})c_2)c_1=(c_1)^{-1}.1.c_1=1$ lo cual pone en evidencia que (c_2c_1) tiene inverso].
Esto pone en evidencia que la relación es **transitiva**.

SE7. **a**) Supongamos que d cumple con las condiciones **i**) , **ii***) de la definición 9, es decir :
1) d es divisor común de a, b ; 2) todo divisor común, h, de a, b necesariamente divide d ;
entonces, si $d^*=d.c$ siendo c unitario, se tiene : $d=(c^{-1})d^*$,
$a=c_1d=c_1(c^{-1})d^*= (c_1(c^{-1}))d^*$, es decir , d^* divide <u>a</u> ; análogamente se verifica que d^* divide a <u>b</u> de manera que d^* también es divisor común de a, b ;
por otra parte, si h es cualquier divisor comun de a, b así que h divide a <u>d</u> de esto sigue que h también divide a d^* ya que se tiene : $h|d \Rightarrow d=h_1h$ por lo cual $d^*=d.c=(h_1h)c = (h_1c)h$.
b) Si d, d^* cumplen con las dos condiciones **i**) , **ii***) entonces :
por cumplir d con las dos condiciones y ser d^* un divisor común de a, b sigue que $d^*|d$;
análogamente, por cumplir d^* con las dos condiciones y por ser d un divisor común de a, b, sigue que $d|d^*$. Por lo tanto d, d^* son asociados y por el ejercicio E4 cada uno es igual al otro multiplicado por un unitario.

SE8. Sea $m*n= (m, n)= M.C.D.(m, n)$. Por la simetría de la definición 9 es evidente que $m*n=n*m$ así que la operación "*" es conmutativa;
usando la observación 6 [ver más adelante] es sencillo verificar que $(a,(b, c)) = ((a, b), c)$, así que la operación "*" es asociativa;
también se puede verificar usando directamente la definición 9, pero es bastante menos sencillo...];
la operación "*" <u>no tiene neutro</u> . Basta observar que si existiese un elemento, e, tal que $n*e=n$, e debería ser múltiplo de n (para todo n), lo cual no es posible.

SE9. $r_1=a$, $r_2=b$; $x_1=1$, $x_2=0$, $y_1=0$, $y_2=1$,
$r_k=r_{k-2}-q_{k-2}.r_{k-1}$;

$x_k=x_{k-2}-q_{k-2}.x_{k-1}$;
$y_k=y_{k-2}-q_{k-2}.y_{k-1}$;

P(n) : $x_k a+y_k b = r_k$;

P(1) : $1.a+0.b=a=r_1$;
P(2) : $0.a+1.b=b = r_2$;

Supongamos ahora cierta la propiedad para todo natural $\leq k$, [$k \geq 2$] y deduzcámosla para k+1 :
$x_{k+1}a+y_{k+1}b =(x_{k-1}-q_{k-1}.x_k)a+(y_{k-1}-q_{k-1}.y_k)b = (x_{k-1}a+y_{k-1}b) - q_{k-1}(x_k a+y_k b) =_{(*)}$
$=r_{k-1}- q_{k-1}r_k= r_{k+1}$.

(*) por hipótesis inductiva .

SE10. $c|a$, $c|b \Rightarrow$ $a=h.c$, $b=k.c$ [h, k$\in$ **D**] luego $sa+tb=shc+tkc = (sh+tk)c$ lo cual implica $c| sa+tb$.

SE11. Se usa cualquiera de los dos métodos que se han considerado :
por ej. (1331, 671) =d =?
1331 = 671.1 +660 ; 671 = 660.1 + 11 ; 660= 66.11+0 ;
d = último resto no nulo = 11 ;
por otra parte : 11 =671- (660. 1) = 671- (1331- 671. 1).1 = 2.671 + (-1).1331;
Con el método demostrado en el ejercicio anterior, [y con referencia a las divisiones que se acaban de efectuar], se tiene :
$r_3=660=r_1- 1.r_2$; $x_3= x_1-1. x_2 = 1-0 = 1$, $y_3=y_1-1.y_2= 0-1=-1$;
$r_4= 11=r_2- 1.r_3$; $x_4 =x_2-1. x_3 = 0- 1.1 = -1$; $y_4=y_2-1.y_3= 1 -(-1) = 2$;
$11= r_4= (x_4a+y_4b) = (-1).1331+2.671$.

SE12. (484, (3993, 2662)) = 121 = 3.484+(-1)3993+1.2662 .

SE13. MCD(30, 42, 70, 105)= (30, (42, (70, 105))) ;
(70, 105)= 35 = (-1).70+1. 105 ;
(42, 35) = 7 = 1.42+(-1).35 = 1.42+(-1) (-70+105)= 1.42+1.70+(-1).105;
(30, 7) = 1 = (-3).30+13.7 = (-3).30 +13.42+13.70+(-13).105 .

SE14. Si b divide : $\underline{c}$, a_1, a_2 entonces $c=c_1b$, $a_1=c_2b$, $a_2=c_3b$ luego
$a_3= c-a_1-a_2 = c_1b-c_2b-c_3b= b(c_1-c_2-c_3)$ lo cual pone en evidencia que $b|a_3$.

SE15. Sea $p|abc=(ab)c$ entonces , por definición de primo [def. 8'] $p|(ab)$ *o* $p|c$; en el caso en que $p|ab$ sigue $p|a$ *o* $p|b$; en definitiva $p|a$ *o* $p|b$ *o* $p|c$.
Observación 15a). En latin , una forma de decir "*o*" era "Vel" así que muchas veces se usa el símbolo "V", inicial de "Vel" para indicar la disyunción "*o*" y por simetría, se usa el símbolo Λ para indicar la conjunción "y" .
El procedimiento anterior entonces se escribiría :
Sea $p|abc=(ab)c$ entonces , por definición de primo [def. 8'] $p|(ab)$ V $p|c$;
en el caso en que $p|ab$ sigue $p|a$ V $p|b$; en definitiva $p|a$ V $p|b$ V $p|c$.

Observación 15b) Una forma equivalente de expresar la proposición :
$p|ab \Rightarrow (p|a \ V \ p|b)$ es : $-(p|a)\Lambda-(p|b) \Rightarrow -(p|ab)$
[indicando con "-r la negación de la proposición r] ;
Esto se puede comprobar usando "tablas de verdad" como se ilustra en la guía opcional sobre "análisis lógico" ; se puede comprobar primero que $r \Rightarrow s$ es equivalente a $(-s) \Rightarrow (-r)$ y luego que $-(qVt)=(-q)\Lambda(-t)$.
Por ejemplo, si r = "n es múltiplo de 4" , s=" n es múltiplo de 2" entonces $r \Rightarrow s$ expresa que todo múltiplo de 4 es múltiplo de 2 , mientras que $(-s) \Rightarrow (-r)$ expresa que si un número no es múltiplo de 2 tampoco es múltiplo de 4 ;
Por otra parte, siempre a título de ejemplo si q= "tengo un perro" , t="tengo un gato" entonces qVt expresa que "tengo un perro *o* un gato" mientras que su negación es equivalente a "no tengo perro" *y* "no tengo gato".
Observación 15c) Tomando en cuenta las dos observaciones anteriores, podemos expresar la definición 8' de número primo con : $-(p|a)\Lambda-(p|b) \Rightarrow -(p|ab)$ lo cual en palabras sería : " el producto de dos números que no son múltiplos de p tampoco es múltiplo de p".
Lo que se pide demostrar en el ejercicio E15 es un caso particular de lo que se pide demostrar en el ejercicio E16 :

SE16. Demuestre por inducción, la propiedad P(n) : si un primo p divide a un producto $a_1a_2...a_n$ de n enteros no nulos, entonces necesariamente p divide a almenos uno de los factores a_i .
P(1) : si $p|a_1$ entonces $p|a_1$ [cierto];
Sea cierto que "si $p|a_1a_2...a_k$ entonces $p|a_i$ para almenos un i $(1 \le i \le k)$ " [esta es la hipótesis inductiva];
P(k+1) : sea $p|a_1a_2...a_ka_{k+1} = (a_1a_2...a_k)a_{k+1}$; entonces por definición de primo $p|a_{k+1}$ o, de no ser así, $p|(a_1a_2...a_k)$ en el cual caso [por hipótesis inductiva] $p|a_i$ para almenos un i $(1 \le i \le k)$; en definitiva $p|a_i$ para almenos un i tal que $1 \le i \le k+1$.
Como hemos verificado que a partir de la hipótesis inductiva se deduce que P(k+1) es cierta, la demostración está hecha.

SE17. Las posibles soluciones racionales de la ecuación $4x^4-3x^2-7x-3 = 0$ son del tipo $\pm\frac{p}{q}$ siendo p un divisor de 3 y siendo q un divisor de 4 , así que debemos averiguar si alguno de los números siguientes anula el polinomio
$P(x) = 4x^4-3x^2-7x-3$:

$$\pm 1 \ , \pm 3 \ , \pm \frac{1}{2} \ , \pm \frac{1}{4} \ , \pm \frac{3}{2} \ , \pm \frac{3}{4} \ ;$$

se verifica que $P(-\frac{1}{2}) = P(\frac{3}{2}) = 0$ por lo cual (2x+1) , (2x-3) son factores del polinomio y se tiene : $4x^4-3x^2-7x-3 = (2x+1)(2x-3)(x^2+x+1)$;
Si consideramos el problema en el conjunto de los números racionales o reales, las soluciones de la ecuación son dos, a saber : $x_1=-\frac{1}{2}$, $x_2=\frac{3}{2}$; si considerásemos el problema en el conjunto de los números complejos, las soluciones serían cuatro :
$x_1=-\frac{1}{2}$, $x_2=\frac{3}{2}$, $x_{3,4} = -\frac{1}{2} \pm \frac{\sqrt{3}\,i}{2}$.

SE18. $\pm 1 , \pm 2 , \pm 4 , \pm \frac{1}{2} , \pm \frac{1}{3} , \pm \frac{2}{3} , \pm \frac{4}{3} , \pm \frac{1}{6}$.

SE19. $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_2 x^2 + a_1 x + a_0$;
si $\frac{p}{q}$ es fracción irreducible, por lo cual (p, q)= 1 y si $f(\frac{p}{q})=0$ entonces :
$f(\frac{p}{q}) = a_n(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + ... + a_2(\frac{p}{q})^2 + a_1(\frac{p}{q}) + a_0 =$
$= \frac{1}{q^n}[a_n p^n + a_{n-1} p^{n-1} q + ... a_2 p^2 q^{n-2} + a_1 p q^{n-1} + a_0 q^n] = 0$ luego :
$a_n p^n + a_{n-1} p^{n-1} q + ... a_2 p^2 q^{n-2} + a_1 p q^{n-1} = - a_0 q^n$; como p divide al primer miembro, p divide al producto $- a_0 q^n$ y como p no divide a q, sigue que $p \mid a_0$.
Análogamente, escribiendo : $- a_n p^n = a_{n-1} p^{n-1} q + ... a_2 p^2 q^{n-2} + a_1 p q^{n-1} + a_0 q^n$ observamos que q divide al segundo miembro, luego q divide a $- a_n p^n$ y como q no divide p sigue que $q \mid a_n$.

SE20. Sea h= producto de los factores primos comunes a m, n con el mínimo exponente;
entonces es evidente que $h \mid m$, $h \mid n$ así que se cumple la condición **i**) de la definición 9;
si h ' es cualquier entero que divide m, n entonces factorizando h ' no puede haber ningún factor primo que no divida ámbos m, n y por otra parte cualquier factor primo de h ' no puede tener exponente mayor que el exponente que tiene el mismo primo en las factorizaciones de m, n; por lo tanto se cumple también la condición **ii***) de la definición 9.

SE21. Recordemos que para garantizar la unicidad del máximo común divisor, d, debemos agregar a las condiciones **i**),**ii***) [ver la observación importante, después de la def. 9]
d > 0 en el caso de los enteros , d = polinomio mónico, en el caso de los polinomios con coeficientes en un cuerpo conmutativo.
Seas d_1, d_2 dos elementos que cumplan con las condiciones **i**), **ii***) respecto a los elementos m, n ;
entonces, por **i**), ámbos dividen m y n ;
por cumplir d_1 con **ii***) y por ser d_2 otro divisor común de m, n deberá ser: $d_2 \mid d_1$;
por cumplir d_2 con **ii***) y por ser d_1 otro divisor común de m, n deberá ser: $d_1 \mid d_2$;
entonces por consiguiente [ver **def.5** y ejercicio **E4**] d_1, d_2 son asociados y cada uno se puede obtener multiplicando al otro por un conveniente elemento unitario;
entonces, si estamos considerando el dominio de integridad de los enteros, será $d_2 = \pm d_1$ y si se exige la condición que el máximo común divisor sea positivo, la única posibilidad es que sea $d_2 = d_1 > 0$;
por otra parte, si estamos considerando el anillo de los polinomios con coeficientes en un cuerpo conmutativo [por ej. el cuerpo de los reales], tenemos $d_2 = u.d_1$ siendo u una constante no nula [ya que en el dominio de integridad de los polinomios con coeficientes en un cuerpo, los elementos unitarios son los polinomios constante no nulos]; en este caso, si se exige la condición que el máximo común divisor sea mónico [recuerde que un polinomio no nulo se llama "mónico" si y sólo si el coeficiente de su monomio de grado máximo es =1] necesariamente u=1 de manera que $d_2 = d_1$.

SE22. Con el mismo método usado en la resolución del ejercicio **E20**,
es fácil verificar que el mínimo común múltiplo de dos enteros [o de dos polinomios] se puede expresar como el producto de todos los factores comunes y no comunes con el máximo exponente.

SE23. **i**)Para comprobar la igualdad (m, n)[m, n] = m.n ;
bastará verificar que los dos miembros tienen exactamente los mismos factores primos con el mismo exponente [teniendo en cuenta los resultados de los ejercicios **E20**, **E22**]
Si p es cualquier elemento primo que se presenta con exponente r en la factorización de m, con exponente s en la factorización de n, [siendo por ej. $0 \leq r \leq s$]
entonces p aparece con exponente r+s en la factorización de mn, con exponente r en la factorización de (m, n) y con exponente s en la factorización de [m, n] por lo cual el exponente de p en la factorización de (m, n)[m, n] también es r+s.
Si todo primo aparece con el mismo exponente [posiblemente nulo] en las factorizaciones de mn y (m, n)[m, n] entonces necesariamente se cumple la igualdad.
A título de ejemplo : sean m=18, n=60 ; el primo p=7 aparece con exponentes r=s=0 en las factorizaciones de 18, 60 así como en las factorizaciones de (18, 60), [18, 60] ;
el primo q=2 aparece con exponente r=1 en las factorizaciones de 18 , (18, 60) , con el exponentes=2 en la factorización de 60 y con el exponente 1+2=3 en la factorización de 18.60=1080 ;
ii) el valor absoluto hace falta en el caso que m, n sean enteros de signo opuesto;
iii) el procedimiento usado en **i)** actúa igual en el dominio de integridad de los polinomios hasta poner en evidencia que, por tener (m, n)[m, n] , m.n los mismos factores primos con los mismos exponentes cada uno de ellos divide al otro, por lo cual son asociados y por consiguiente uno se obtiene multiplicando al otro por un conveniente unitario.

SE24. La sugerencia lo dice todo...

SE25. a=3000 , b=8751;
Con el algoritmo de la división de Euclides tenemos :
8751 = 2.3000+2751;
3000=1.2751+249;
2751=11.249+12;
249=20.12+9;
12=1.9+3; 9=3.3+0. El último resto no nulo es
r_7=3 = (8751, 3000) = 12- 9 = 12- (249-20.12)=21.12- 249 =
= 21.(2751-11.249) - 249 = 21.2751-232.249=21.2751-232(3000-2751) =
= 253.2751-232.3000= 253(8751-2.3000)-232.3000=253(8751)-738(3000);
por lo tanto 81=27.3=27[253(8751)-738(3000)]=6831(8751)- 19926(3000) .

SE26. si existen s, t tales que sa+tb=k entonces existen infinitos pares de números s', t' con la misma propiedad, ya que si restamos miembro a miembro las dos igualdades: sa+tb=k , s'a+t'b=k obtenemos : (s-s ')a+(t-t ')b=0 por lo cual si h es cualquier entero, con las fórmulas s ' = s-hb , t '=t+ha podemos obtener infinitos pares de números con la propiedad deseada. En particular es posible escoger el entero h de manera que sea s ' =s-hb < 0.

SE27. **a**) **cierto**. Se puede justificar usando el resultado del ejercicio **E22** ;
b) **cierto**. Sea d=(m, n) y sea k=ad ;
por definición de MCD :
por la condición **i**) d divide ámbos, m,n luego $m=m_1d$, $n = n_1d$; así que
$am=m_1k$, $an=n_1k$ por lo cual k es divisor común de am, an y cumple
con la condición **i**);
si k ' es divisor común de am, an , es decir $am=m_2k'$, $an=n_2k'$ entonces, teniendo en cuenta que d=combinación lineal de m, n = sm+tn y por consiguiente
$k=ad=a(sm+tn) =s(m_2k')+t(n_2k')=(sm_2+tn_2)\,k'$ resulta que $k' \mid k$ es decir, k cumple también con la condición **ii***).
Nota : la parte **b**) también se puede justificar usando la definición mencionada en la **observación 6** ;
c) **cierto**. Obviamente $1 \mid h$, $1 \mid k$, así que falta verificar que cualquier divisor común de h, k es unitario [±1 en el caso de los enteros, constante no nula, en el caso de los polinomios] .
Sea s un divisor común de h, k, entonces se tiene $h=h_1s$, $k=k_1s$; por otra parte, $d=am+bn = adh+bdk$ por lo cual $ah+bk=1$ y también $ah_1s+k_1sb = 1=s(ah_1+k_1b)$ de lo cual sigue que s es unitario [y por lo tanto $s \mid 1$, es decir se cumple **ii***)] .

SE28. La sugerencia lo dice todo...

SE29. Sea $p_1p_2= q_1q_2q_3$, siendo p_1, p_2, q_1, q_2, q_3 primos.
Entonces , por la propiedad ilustrada en la "aplicación 1" después del ejercico **E14** , como q_3 divide al producto p_1p_2 , necesariamente debrá dividir a uno de los dos factores, por ejemplo $q_3 \mid p_2$; entonces $p_2= a.q_3$ y esta factorización , por ser p_2 primo, es impropia, así que uno de los dos factores debe ser unitario [y como q_3 por ser primo no es unitario, sigue que a es unitario]; se tiene entonces [con a unitario] :
$p_1p_2=p_1a.q_3= q_1q_2q_3$ de lo cual sigue $p_1a = q_1q_2$; con un análogo procedimiento se deduce que $p_1=b.q_2$, con b unitario y de esto sigue : $ab= q_1$ lo cual no puede ser ya que ab es unitario y q_1 primo (no unitario).

SE30. Como todo divisor común de a, b divide a-b, a+b, se tiene que d=(a, b) debe dividir a d*=(a+b, a-b); inversamente, todo divisor común de a-b, a+b dividirá $2a=(a-b)+(a+b)$, $2b=(a+b)-(a-b)$ y dividirá también a su MCD es decir a (2a, 2b) = 2d [ver ejercicio **E27b**.]; por lo tanto tenemos :

$$d \mid d^* \ , \ d^* \mid 2d \ ;$$

i) si a, b no tienen la misma paridad, entonces ámbos, d, d* son impares y $d^* \mid 2d$ implica $d^* \mid d$ de manera que d, d* son asociados y como ámbos son positivos d=d* .
Recordar "aplicación 2" después del ejercicio **E14** : $d^* \mid 2d$ significa $2d=cd^*$ y como 2, d* no tienen factores comunes, sigue que (2, d*)=1 y existen enteros s, t tales que $2s+td^*=1$, luego $d=d.1=d(2s+td^*)= s(2d)+dtd^*=$
$=scd^*+dtd^*=d^*(sc+dt)$,es decir $d^* \mid d$;
ii) por ejemplo, si a=15, b=27 se tiene (15, 27)=3 ; (15+27, 15-27)=(42, - 12)= 6;

iii) Es posible : por ejemplo : (8, 6)= 2 ; (8+6, 8-6)=(14, 2) = 2;
no es posible nunca, en el caso que a, b sean ámbos impares, ya que en este caso siempre d=(a, b) es impar, mientras que (a+b, a-b) es par ya que la suma y la resta de dos números impares es par.