TEMAS DE MATEMÁTICAS
(OPOSICIONES DE SECUNDARIA)

TEMA 4

NÚMEROS ENTEROS. DIVISILIBIDAD. NÚMEROS PRIMOS. CONGRUENCIA.

1. Introducción.
2. Los Números Enteros.
   2.1. Construcción de $\mathbb{Z}$.
   2.2. El Grupo Aditivo de los Números Enteros.
   2.3. El Semigrupo Multiplicativo de los Números Enteros.
   2.4. El Anillo de los Números Enteros.
   2.5. Ideales en el Anillo de los Números Enteros.
3. Divisibilidad.
   3.1. Divisibilidad de Números Enteros.
   3.2. Divisibilidad en el Anillo de los Números Enteros.
   3.3. Máximo Común Divisor y Mínimo Común Múltiplo.
4. Números Primos.
5. Congruencias.
6. Criterios de Divisibilidad.

Bibliografía Recomendada.

TEMA 4

NÚMEROS ENTEROS. DIVISILIBIDAD. NÚMEROS PRIMOS. CONGRUENCIA.

1. INTRODUCCIÓN.

Este tema se divide en cinco partes fundamentales. La primera parte son Los Números Enteros. Comenzaremos definiendo el conjunto de los números enteros. Definiremos en él la operación de suma, que lo convertirá en grupo abeliano. Luego la operación producto, constituyendo un grupo multiplicativo abeliano con elemento unidad. Ambas operaciones nos crearán el anillo de los números enteros. Y al final trataremos de los ideales en el anillo, que se caracterizan por ser subconjuntos formados por los múltiplos de un número entero.

La segunda parte es la Divisibilidad. La divisibilidad en el anillo de los números enteros se define de forma precisa en términos de ideales. Por último veremos la existencia y unicidad del Máximo Común Divisor y Mínimo Común Múltiplo.

En la tercera parte definiremos los números primos y veremos sus propiedades. Aquí hemos de resaltar el teorema fundamental de la aritmética.

En la cuarta parte trataremos con congruencias y en la última veremos los criterios de divisibilidad más importantes.

2. LOS NÚMEROS ENTEROS.

En el tema 1 definimos el conjunto de los números naturales, el cual tiene estructura de Semianillo conmutativo. Ahora tenemos que ampliar dicho conjunto. El motivo es que ecuaciones del tipo $x+m=n$ donde se verifica que $m>n$ no tendrían solución. Por tanto, hemos de construir un nuevo conjunto en el cual esas ecuaciones siempre tengan solución. Ese conjunto ha de estar dotado de una operación interna (suma) que sea extensión de la operación interna de $\mathbb{N}$ y que verifique que todo elemento tiene simétrico.

2.1. Construcción de $\mathbb{Z}$.

DEF Sea el conjunto $\mathbb{N}\times\mathbb{N}=\{(a,b) / a\in\mathbb{N}, b\in\mathbb{N}\}$. Sobre este conjunto definimos la relación R

$$(a,b)R(c,d) \Leftrightarrow a+d = b+c$$

PROP La relación R es una relación de equivalencia.

Dem.

Para que R sea una relación de equivalencia, debe verificar las propiedades reflexiva, simétrica y transitiva.

a) Reflexiva. $a+b=b+a$ ya que $\mathbb{N}$ es conmutativo $\Rightarrow (a,b)R(a,b)$

b) Simétrica $(a,b)R(c,d) \Rightarrow a+d=b+c \Rightarrow b+c=a+d \Rightarrow$

Aplicando la conmutatividad $c+b=d+a \Rightarrow (c,d)R(a,b)$

c) Transitividad

$(a,b)R(c,d) \Rightarrow a+d=b+c$

$(c,d)R(e,f) \Rightarrow c+f=d+e$

Sumando ambas expresiones miembro a miembro

$$a+d+c+f=b+c+d+e \quad \Rightarrow \quad a+f=b+e \quad \Rightarrow \quad (a,b)R(e,f)$$

Por tanto R es una relación de equivalencia.

COROLARIO La relación R sobre $\mathbb{N}x\mathbb{N}$ define un conjunto cociente cuyos elementos son las clases de equivalencia [(a,b)] donde

$$[(a,b)]=\{(m,n)\in \mathbb{N}x\mathbb{N} / (m,n)R(a,b)\}$$

DEF Se define el conjunto de los números enteros, y lo representamos por $\mathbb{Z}$, como el conjunto cociente $\mathbb{N}x\mathbb{N}/R$. Es decir $\mathbb{Z}=\mathbb{N}x\mathbb{N}/R$

OBS Sabemos que toda clase de equivalencia queda determinada dando un representante cualquiera de la misma. Por convenio, los representantes de las clases de equivalencia serán aquellos pares ordenados que tengan al menos una de sus componentes nula.

Se pueden dar tres casos, dado $(a,b)\in \mathbb{N}x\mathbb{N}$

1) $a>b$

En este caso existe $m\in \mathbb{N}$ tal que $a=b+m$. Entonces se verifica $(a,b)R(m,0)$. Todos los elementos de $[(m,0)]$ son de la forma $[(m,0)]=\{(b+m,b) / b\in \mathbb{N}\}$.

Al representante de $[(m,0)]$ lo denotaremos con el símbolo $+m$, o simplemente, m. El conjunto $\mathbb{Z}^+=\{[(m,0)] / m\in \mathbb{N}\}$ lo llamaremos conjunto de los números enteros positivos.

2) $a<b$

Existe $n\in \mathbb{N}$ tal que $a+n=b$. Se verifica $(a,b)R(0,n)$. Todos los elementos de $[(0,n)]$ son de la forma $[(0,n)]=\{(a,a+n) / a\in \mathbb{N}\}$.

Al representante de $[(0,n)]$ lo denotaremos con el símbolo $-n$. El conjunto $\mathbb{Z}^-=\{[(0,n)] / n\in \mathbb{N}\}$ se llamará conjunto de los números enteros negativos.

3) a=b

Se verifica que (a,b)R(0,0). Todos los elementos de [(0,0)] son de la forma [(0,0)]={(a,a) / a∈ℕ}.

Al representante de [(0,0)] lo denotaremos con el símbolo 0.

Ahora ya estamos en condiciones de afirmar que $\mathbb{Z}=\mathbb{Z}^+\cup\{0\}\cup\mathbb{Z}^-$

PROP El conjunto ℤ es una extensión de ℕ.

Dem.

Basta ver que $\mathbb{N}\subset\mathbb{Z}$ lo cual es evidente ya que $0\in\mathbb{N}\Rightarrow 0\in\mathbb{Z}$

$\forall n\in\mathbb{N}-\{0\}\Rightarrow [(n,0)]\in\mathbb{Z}^+\subset\mathbb{Z}$

2.2. El Grupo Aditivo de los Números Enteros.

Vamos a definir en ℤ la suma para dotarlo de estructura de grupo.

DEF Definimos la suma en ℤ como

$$+: \mathbb{Z}x\mathbb{Z}\rightarrow\mathbb{Z}$$

con $(a,b)x(c,d)\in\mathbb{Z}x\mathbb{Z}$, entonces +((a,b),(c,d))=(a+c,b+d)

Notación: La expresión +((a,b),(c,d)) se representa por (a,b)+(c,d).

PROP La suma así definida no depende del representante elegido.

Dem.

Sean (a,b)R(a',b') y (c,d)R(c',d')

Para ver que [(a,b)+(c,d)]=[(a',b')+(c',d')]

tendremos que probar que ((a,b)+(c,d))R((a',b')+(c',d'))

$$(a,b)R(a',b')\Rightarrow a+b'=a'+b$$

$$(c,d)R(c',d')\Rightarrow c+d'=c'+d$$

sumando ambas expresiones miembro a miembro

$$a+c+b'+d' = a'+c'+b+d \Rightarrow (a+c,b+d)R(a'+c',b'+d') \Rightarrow$$

$$\Rightarrow ((a,b)+(c,d))\ R\ ((a',b')+(c',d'))$$

PROP La operación de suma definida anteriormente verifica las siguientes propiedades:

1) Asociativa: $[(a,b)]+([(c,d)]+[(e,f)])=([(a,b)]+[(c,d)])+[(e,f)]$
2) Conmutativa: $[(a,b)]+[(c,d)]=[(c,d)]+[(a,b)]$
3) Elemento Neutro: $[(0,0)]$, ya que $[(a,b)]+[(0,0)]=[(a,b)]=[(0,0)]+[(a,b)]$
4) Elemento Opuesto: $\forall[(a,b)]\ \exists[(b,a)]$ tal que $[(a,b)]+[(b,a)]=[(0,0)]$

Dem.

1) $[(a,b)]+([(c,d)]+[(e,f)]) = [(a,b)]+([(c+e,d+f)]) = [(a+(c+e),b+(d+f))] =$

$= [((a+c)+e,(b+d)+f)] = [(a+c,b+d)]+[(e,f)] = ([(a,b)]+[(c,d)])+[(e,f)]$

2) $[(a,b)]+[(c,d)] = [(a+c,b+d)] = [(c+a,d+b)] = [(c,d)]+[(a,b)]$

3) $[(a,b)]+[(0,0)] = [(a+0,b+0)] = [(a,b)]$

$[(0,0)]+[(a,b)] = [(0+a,0+b)] = [(a,b)]$

Por lo tanto $[(0,0)]$ es el elemento neutro y se representa por 0

4) $\forall[(a,b)]$ $[(a,b)]+[(b,a)] = [(a+b,b+a)] = [(0,0)]$

Luego el opuesto de $[(a,b)]$ es $[(b,a)]$

Es el llamado elemento simétrico con respecto a la operación de suma.

PROP El simétrico de cada número es único.

Dem.

Sea $[(a,b)]$. Supongamos que admite dos simétricos: $[(b,a)]$ y $[(c,d)]$

$[(a,b)]+[(b,a)] = [(0,0)] = [(a,b)]+[(c,d)] \Rightarrow [(a+b,b+a)] = [(a+c,b+d)]$

Y para que las clases sean iguales, sus elementos han de estar relacionados:

$$(a+b,b+a)\ R\ (a+c,b+d)$$

lo que significa que $a+b+b+d = b+a+a+c$

Aplicando la ley de simplificación en $\mathbb{N}$ $b+d = a+c$

y eso es $(b,a)\ R\ (c,d)$

y por tanto $[(b,a)] = [(c,d)]$

y ambos elementos son el mismo.

OBS En general $\forall n \in \mathbb{Z}$, se designa a su simétrico por –n

Como conclusión, la operación suma definida junto con las operaciones que hemos comprobado que verifica, nos indican que $(\mathbb{Z},+)$ es un Grupo Abeliano.

Una consecuencia de la definición de suma, y por ser $(\mathbb{Z},+)$ un grupo, se verifica la propiedad cancelativa en la suma de números enteros.

PROP $\forall p,q,r \in \mathbb{Z}.\ p+q=p+r \Rightarrow q=r$

Dem.

Como $p \in \mathbb{Z} \Rightarrow \exists (-p) \in \mathbb{Z} / p+(-p)=0$

$$p+q=p+r \Rightarrow (-p)+(p+q) = (-p)+(p+r) \Rightarrow$$

Aplicando la propiedad asociativa $((-p)+p)+q = ((-p)+p)+r \Rightarrow$

Aplicando la propiedad de existencia de opuesto $0+q = 0+r \Rightarrow$

Aplicando la propiedad de existencia de neutro $q=r$

Ahora que ya tenemos a $(\mathbb{Z}.+)$ como grupo podemos afirmar:

1) Existe una operación inversa a la adición, que llamaremos diferencia.

$$\forall m,n \in \mathbb{Z} \quad m-n = m+(-n)$$

2) La ecuación $x+m=n$ con $m,n \in \mathbb{Z}$ es resoluble en $\mathbb{Z}$, siendo la solución $x=n+(-m)$ y es única.

DEF Se define la sustracción o resta de números enteros como la suma del primero con el opuesto del segundo. m-n = m+(-n)

Esta operación es interna en $\mathbb{Z}$, pero no verifica las propiedades conmutativa y asociativa.

Veamos que la suma de números enteros se corresponde con la construcción que hicimos de $\mathbb{Z}$:

1) $+m+n = [(m,0)]+[(n,0)] = [(m+n,0)] = +(m+n)$

2) $–m+(-n) = [(0,m)]+[(0,n)] = [(0,m+n)] = -(m+n)$

3) $+m+(-n) = [(m,0)]+[(0,n)] = [(m,n)]$

   a) Si $m>n \Rightarrow [(m,n)] = +(m-n)$

   b) Si $m<n \Rightarrow [(m,n)] = -(n-m)$

   c) Si $m=n \Rightarrow [(m,n)] = 0$

2.3. El Semigrupo Multiplicativo de los Números Enteros.

Vamos a definir en $\mathbb{Z}$ una operación producto tal que $(\mathbb{Z},\cdot)$ sea un semigrupo conmutativo con elemento unidad, prolongando el producto definido en $\mathbb{N}$.

DEF Definimos la multiplicación de números enteros como:

$$\cdot : \mathbb{Z}x\mathbb{Z} \to \mathbb{Z}$$

con $(a,b)x(c,d) \in \mathbb{Z}x\mathbb{Z}$, entonces $\cdot((a,b),(c,d))=(ac+bd,ad+bc)$

Notación: La expresión $\cdot((a,b),(c,d))$ se representa por $(a,b)\cdot(c,d)$.

PROP El producto así definido no depende de los representantes elegidos.

Dem.

Sean $(a,b)R(a',b')$ y $(c,d)R(c',d')$

Para ver que $[(a,b)\cdot(c,d)]=[(a',b')\cdot(c',d')]$

tendremos que probar que $((a,b)\cdot(c,d))R((a',b')\cdot(c',d'))$

que es equivalente a $ac+bd+a'd'+b'c' = ad+bc+a'c'+b'd'$

Vamos a ver que se verifica esa igualdad en dos pasos:

Paso 1:

Comprobar: $(a,b)R(a',b')$ y $(c,d)R(c,d) \Rightarrow (a,b)\cdot(c,d)\ R\ (a',b')\cdot(c,d)$

$$ac+bd+a'd+b'c = (a+b')c+(b+a')d =$$

Como $(a,b)R(a',b') \Rightarrow a+b'=b+a'$

$$= (b+a')c+(a+b')d = ad+bc+a'c+b'd$$

Uniendo ambos extremos: $ac+bd+a'd+b'c = ad+bc+a'c+b'd$

Que es lo mismo que $(a,b)\cdot(c,d)\ R\ (a',b')\cdot(c,d)$

Paso 2:

Comprobar: $(a',b')R(a',b')$ y $(c,d)R(c',d') \Rightarrow (a',b')\cdot(c,d)\ R\ (a',b')\cdot(c',d')$

La demostración de este paso es análoga a la anterior.

Como la relación R es transitiva, tenemos que:

$$(a,b)\cdot(c,d)\ R\ (a',b')\cdot(c,d) \text{ y } (a',b')\cdot(c,d)\ R\ (a',b')\cdot(c',d') \Rightarrow$$

$$\Rightarrow (a,b)\cdot(c,d)\ R\ (a',b')\cdot(c',d')$$

que era lo que queríamos comprobar.

PROP La multiplicación de números enteros cumple las siguientes propiedades:

1) Asociativa: $\forall m,n,p\in\mathbb{Z}$ $(m\cdot n)\cdot p=m\cdot(n\cdot p)$

2) Conmutativa: $\forall m,n\in\mathbb{Z}$ $m\cdot n=n\cdot m$

3) Elemento Neutro: $\exists e\in\mathbb{Z}\ \ \forall m\in\mathbb{Z}$ $m\cdot e=m=e\cdot m$ siendo $e=1$

Dem.

Sea m un representante de la clase [(a,b)], n de [(c,d)], p de [(e,f)] y e de $[(e_1,e_2)]$

1) $(m\cdot n)\cdot p = ([(a,b)]\cdot[(c,d)])\cdot[(e,f)] = [(ac+bd\ ,\ ad+bc)]\cdot[(e,f)] =$

$= [((ac+bd)e+(ad+bc)f\ ,\ (ac+bd)f+(ad+bc)e)] =$

$= [(ace+bde+adf+bcf\ ,\ acf+bdf+ade+bce)] =$

$= [(a(ce+df)+b(de+cf)\ ,\ a(cf+de)+b(df+ce))]$

$= [(a,b)]\cdot[(ce+df\ ,\ de+cf)] = [(a,b)]\cdot([(c,d)]\cdot[(e,f)]) = m\cdot(n\cdot p)$

2) $m\cdot n=[(a,b)]\cdot[(c,d)]=[(ac+bd,\ ad+bc)]=[(ca+db,\ da+cb)]=[(c,d)]\cdot[(a,b)]=n\cdot m$

3) $m\cdot e=m \Rightarrow [(a,b)]\cdot[(e_1,e_2)]=[(a,b)] \Rightarrow \left.\begin{matrix} ae_1+be_2=a \\ ae_2+be_1=b \end{matrix}\right\} \Rightarrow$

Para resolver el sistema de ecuaciones multiplicamos la primera por a y la segunda por b

$$\Rightarrow \left.\begin{matrix} a^2e_1+abe_2=a^2 \\ abe_2+b^2e_1=b^2 \end{matrix}\right\} \Rightarrow$$

restando ambas ecuaciones: $a^2e_1-b^2e_1=a^2-b^2 \Rightarrow e_1=1$

sustituyendo en la primera ecuación obtenemos $e_2=0$

Luego $e=[(1,0)]=1\in\mathbb{Z}$

Por conmutatividad $m\cdot e=e\cdot m$

Ya estamos en condiciones de poder afirmar que $(\mathbb{Z},\cdot)$ es un semigrupo conmutativo con elemento unidad.

PROP Otras propiedades del producto de números enteros son:

1) Ley de Simplificación: $\forall m,n,p\in\mathbb{Z}-\{0\}$, si $m\cdot n=m\cdot p \Rightarrow n=p$

2) El cero es un elemento absorbente: $\forall m\in\mathbb{Z}\ \ m\cdot 0=0$

3) $\mathbb{Z}$ no posee divisores de cero: $\forall m,n\in\mathbb{Z}$, si $m\cdot n=0 \Rightarrow m=0$ ó $n=0$

Dem:

A demostrar por el lector

OBS Teniendo en cuenta la definición que hemos dado de números enteros (tanto positivos como negativos) y la definición de producto, podemos obtener la Regla de los Signos:

1) $+m\cdot+n=[(m,0)]\cdot[(n,0)]=[(m\cdot n,0)]=+(m\cdot n)$

2) $+m\cdot(-n)=[(m,0)]\cdot[(0,n)]=[(0,m\cdot n)]=-(m\cdot n)$

3) $-m\cdot+n=[(0,m)]\cdot[(n,0)]=[(0,m\cdot n)]=-(m\cdot n)$

4) $-m\cdot(-n)=[(0,m)]\cdot[(0,n)]=[(m\cdot n,0)]=+(m\cdot n)$

PROP Propiedad distributiva del producto respecto de la suma:

$\forall m, n, p \in \mathbb{Z}$ 1) $m\cdot(n+p)=m\cdot n+m\cdot p$ (por la izq.)
2) $(m+n)\cdot p=m\cdot p+n\cdot p$ (por la der.)

Dem

Como ambas demostraciones son análogas, sólo haremos una:

1) Sea *m* un representante de la clase [(a,b)], *n* de la clase [(c,d)] y *p* de [(e,f)]

$m\cdot(n+p)=[(a,b)]\cdot([(c,d)]+[(e,f)])=[(a,b)]\cdot[(c+e,d+f)]=$

$=[(a\cdot(c+e)+b\cdot(d+f), a(d+f)+b(c+e)]=[(ac+ae+bd+bf, ad+af+bc+be)]=$

$=[(ac+bd+ae+bf, ad+bc+af+be)]=[(ac+bd, ad+bc)]+[(ae+bf, af+be)]=$

$=[(a,b)]\cdot[(c,d)]+[(a,b)]\cdot[(e,f)]= m\cdot n+m\cdot p$

PROP El conjunto $\mathbb{Z}$, con las operaciones de suma y producto definidas es una extensión de $\mathbb{N}$, con sus dos operaciones de suma y producto.

Dem

Definamos la aplicación $f: \mathbb{N}\to\mathbb{Z}$ con $f(n)=+n$

Es fácil comprobar que: $f(m+n)=f(m)+f(n)$

y $f(m\cdot n)=f(m)\cdot f(n)$ $\forall m,n\in \mathbb{N}$

Basta tener en cuenta la definición de suma y producto en $\mathbb{Z}$.

2.4. Anillo de los Números Enteros.

Como $(\mathbb{Z},+)$ es un grupo abeliano, $(\mathbb{Z},\cdot)$ es un semigrupo conmutativo con elemento unidad y se verifica la propiedad distributiva por ambos lados, entonces $(\mathbb{Z},+,\cdot)$ tiene estructura de Anillo Conmutativo unitario.

Veamos algunas de las propiedades de $(\mathbb{Z},+,\cdot)$

PROP El anillo de los números enteros no posee divisores de cero. Es decir:

$$\forall m,n\in\mathbb{Z} \qquad \text{Si } m\cdot n=0 \Rightarrow m=0 \text{ ó } n=0$$

DEF $(\mathbb{Z},+,\cdot)$ es un dominio de integridad, ya que es un anillo conmutativo con elemento unidad y sin divisores de cero.

PROP El cero es un elemento absorbente. Es decir: $\forall a\in\mathbb{Z}$ $a\cdot 0=0\cdot a=0$

Dem

Sabemos que $\forall b\in\mathbb{Z}$ se verifica que $b+0=0+b=b$

Teniendo en cuenta esto: $a\cdot b=a\cdot(b+0)=a\cdot b+a\cdot 0$

Aplicando la ley simplificativa: $0=a\cdot 0$

De forma análoga para : $0=0\cdot a$

PROP $\forall a,b\in\mathbb{Z} \Rightarrow a\cdot(-b)=-(a\cdot b)=(-a)\cdot b$

Dem

Sabemos que $\forall b\in\mathbb{Z}$ $\exists(-b)\in\mathbb{Z}$ / $b+(-b)=0$

$$b+(-b)=0 \Rightarrow a\cdot[b+(-b)]=a\cdot 0 \Rightarrow ab+a(-b)=0 \Rightarrow a\cdot(-b)=-(ab)$$

De forma análoga se comprueba que $(-a)\cdot b=-(ab)$

PROP $\forall a\in\mathbb{Z}$ $(-a)\cdot(-b)=ab$

2.5 Ideales en el Anillo de los Números Enteros.

Sabemos que $\mathbb{Z}$ es un anillo conmutativo unitario y además es un dominio de integridad, ya que no posee divisores de cero.

Vamos a definir ahora el concepto de *ideal.*

DEF Sea I un subconjunto de $\mathbb{Z}$. Se dice que I es un ideal de $\mathbb{Z}$ si verifica:

a) I es un subgrupo aditivo de $\mathbb{Z}$.

b) $\forall a \in \mathbb{Z} \quad \forall x \in I$ se cumple $a \cdot x \in I$

OBS El subgrupo de $\mathbb{Z}$ formado por todos los múltiplos de un entero cualquiera $m \in \mathbb{Z}$ es un ideal de $\mathbb{Z}$. La comprobación es trivial.

El ideal lo representamos por (m).

Ya que los múltiplos de *m* coinciden con los de (-m), por convenio, al hablar del ideal (m) tomaremos un positivo.

Comprobemos que todo ideal de $\mathbb{Z}$ es de la forma (m).

PROP Dado un ideal I de $\mathbb{Z}$, se verifica que I=(m) para un entero *m* convenientemente elegido.

Dem

Por ser I un ideal, se verifica $I \subset \mathbb{Z}$.

Si I=(0), la proposición queda demostrada.

Supongamos pues que $I \neq (0)$. Entonces I deberá contener enteros positivos. Sea *m* el menor de los enteros positivos de I. Comprobemos que I=(m), y lo haremos por doble inclusión.

$(m) \subset I$ Como $m \in I$ e I es un ideal $\Rightarrow$ $(m) \subset I$

$I \subset (m)$ Supongamos que $I \not\subset (m)$ y llagaremos a una contradicción.

Como $I \not\subset (m) \Rightarrow \exists a \in (m) / a \in (m)$

Si dividimos *a* por *p* obtenemos: $a = m \cdot q + r$ con $r < m$

Si $r=0 \Rightarrow a = mq \Rightarrow a \notin (m)$ Falso luego $0 < r < m$

Sea el número entero $r = a - mq$

Como $a \in I$, $m \in I \Rightarrow a - mq \in I \Rightarrow r \in I$

Pero $r < m$ y m era el entero positivo más pequeño de I. Contradicción.

La suposición es falsa y $I \subset (m)$

El subconjunto constituido por el elemento 0 es un ideal y se llama, ideal 0, y se designa por (0). Como $\mathbb{Z}$ posee elemento unidad, se verifica que $(1) = \mathbb{Z}$

Los ideales (0) y (1) se llaman ideales impropios. Los restantes, si existen, se llaman *ideales propios.*

DEF Sea I un ideal. Diremos que I es un ideal principal si está engendrado por un solo elemento.

COROLARIO Todo ideal de $\mathbb{Z}$ es un ideal principal.

DEF (a) es un subideal de (b) si $(a)\subset(b)$

Con los ideales de $\mathbb{Z}$ podemos definir las operaciones de suma e intersección de ideales, dando como resultado un nuevo ideal.

PROP 1) $(a)+(b)=\{p\in\mathbb{Z} / p=m+n, m\in(a), n\in(b)\}$ es un ideal

2) $(a)\cap(b)=\{p\in\mathbb{Z} / z\in(a) \text{ y } z\in(b)\}$ es un ideal

Dem

1) Sean $m,n\in(a)+(b) \Rightarrow m=a_1+b_1$ y $n=a_2+b_2$ con

$$a_1,a_2\in(a) \text{ y } b_1,b_2\in(b)$$

$$m-n=(a_1+b_1)-(a_2+b_2)=(a_1-a_2)+(b_1-b_2)$$

Como: $a_1-a_2\in(a)$ y $b_1-b_2\in(b)$ por ser (a) y (b) ideales se verifica que:

$$m-n\in(a)+(b) \qquad (1)$$

Sea $n\in(a)+(b) \Rightarrow n=a_1+b_1$ con $a_1\in(a)$ y $b_1\in(b)$

$$\forall c\in\mathbb{Z} \quad c.n=c(a_1+b_1) \Rightarrow c.n=ca_1+cb_1$$

Se verifica que $ca_1\in(a)$ y $cb_1\in(b)$

entonces: $c.n\in(a)+(b) \qquad (2)$

De (1) y (2) se deduce que (a)+(b) es un ideal.

2) Sean $m,n\in(a)\cap(b) \Rightarrow m,n\in(a)$ y $m,n\in(b) \Rightarrow m-n\in(a)$ y $m-n\in(b) \Rightarrow$

$$\Rightarrow m-n\in(a)\cap(b) \qquad (1)$$

Sea $n\in(a)\cap(b)$ y $c\in\mathbb{Z} \Rightarrow$ Como $n\in(a)$ y $n\in(b)$ se verifica que:

$$n.c\in(a) \text{ y } n.c\in(b) \Rightarrow n.c\in(a)\cap(b) \qquad (2)$$

De (1) y (2) se deduce que $(a)\cap(b)$ es un ideal.

Veamos ahora algunos ideales especiales

DEF Diremos que un ideal I es primo si verifica:

1) $I \neq \mathbb{Z}$

2) $n \cdot n \in I \Rightarrow m \in I$ ó $n \in I$.

PROP I=(m) es un ideal primo de $\mathbb{Z}$ si y sólo si *m* es un número primo.

Dem

OBS Como $\mathbb{Z}$ es un dominio de integridad, los ideales impropios son primos y por tanto los excluiremos de la demostración.

"$\Rightarrow$"

Demostrar: (m) es ideal primo $\Rightarrow$ (m) es número primo.

Es equivalente a: m no es número primo $\Rightarrow$ (m) no es ideal primo.

Si m no es un número primo $\Rightarrow \exists a,b \in \mathbb{Z}$ / $m=a+b$ con $a \neq \pm 1$ y $b \neq \pm 1$.

Podemos considerar a y b positivos, luego: $m \in (m)$ y $m=a \cdot b$

Pero $a \notin (m)$ y $b \notin (m)$ ya que *m* es el entero positivo más pequeño. Por tanto (m) no es primo al no verificar la segunda condición de la definición.

"$\Leftarrow$"

Sea *m* un número primo y $a \cdot b \in (m) \Rightarrow a \cdot b = r \cdot m$

Como *m* es primo, debería dividir a *a* o *b* $\Rightarrow a \in (m)$ ó $b \in (m)$

DEF Diremos que un ideal M es maximal si verifica:

1) $M \neq \mathbb{Z}$

2) $\forall I \in \mathbb{Z}$ ideal y $M \subset I \Rightarrow I=\mathbb{Z}$ ó $I=M$

DEF Llamaremos números primarios a los números de la forma p^n con p primo y $n \in \mathbb{N}^*$ ($\mathbb{N}^*=\mathbb{N}-\{0\}$)

DEF Los ideales primarios de $\mathbb{Z}$ son los generados por el 0 y las potencias positivas de los números primos.

3. DIVISIBILIDAD.

3.1. Divisibilidad de Números Enteros.

DEF Sean $a,b\in\mathbb{Z}$, diremos que "*a* divide a *b*" o "*a* es un divisor de *b*" ó "*b* es un múltiplo de *a*" y lo denotaremos por ser a/b ó b= & si:

$$\exists c\in\mathbb{Z} \,/\, b=a\cdot c$$

OBS A partir de la definición es fácil comprobar que:

1) 1/a $\forall a\in\mathbb{Z}$ 1/a ya que $\exists a\in\mathbb{Z} \,/\, a=1\cdot a$

2) a/0 $\forall a\in\mathbb{Z}$ a/0 ya que $\exists 0\in\mathbb{Z}$ y se verifica $0=a\cdot 0$

PROP $\forall a,b,c\in\mathbb{Z}$ se verifica:

1) $\forall a\in\mathbb{Z}$ a/a

2) Si a/b y b/c $\Rightarrow$ a/c

3) Si a/b y b/a $\Rightarrow$ $a=\pm b$

Dem

1) $\forall a\in\mathbb{Z}$ $\exists 1\in\mathbb{Z} \,/\, a=1\cdot a$

2) Si a/b $\Rightarrow$ $\exists n_1\in\mathbb{N} \,/\, b=a\cdot n_1$
Si b/c $\Rightarrow$ $\exists n_2\in\mathbb{N} \,/\, c=b\cdot n_2$
$\Rightarrow$ $c=(a\cdot n_1)\cdot n_2$; $c=a(n_1\cdot n_2)$

Como: $n_1\cdot n_2\in\mathbb{Z} \Rightarrow$ a/c

3) Si a/b $\Rightarrow$ $\exists n_1\in\mathbb{N} \,/\, b=a\cdot n_1$
Si b/a $\Rightarrow$ $\exists n_2\in\mathbb{N} \,/\, a=b\cdot n_2$
$\Rightarrow$ $a=b\cdot\cdot n_2$; $a=(a\cdot n_1)\cdot n_2$

$\Rightarrow$ $a=a\cdot(n_1\cdot n_2)$ $\Rightarrow$ $a=a\cdot(n_1\cdot n_2)=0$ $\Rightarrow$ $a(1-n_1\cdot n_2)=0$

Si a=0 $\Rightarrow$ como $b=a\cdot n_1$ tenemos b=0

Si $a\neq 0$ $\Rightarrow$ $1-n_1\cdot n_2=0$ por ser $\mathbb{Z}$ un dominio de integridad $\Rightarrow$

$\Rightarrow$ $n_1\cdot n_2=1$ $\Rightarrow$ $n_1=n_2=1$ ó $n_1=n_2=-1$

Se deduce pues que $a=b$ ó $a=-b$

Si consideramos el par $(\mathbb{Z},/)$, vemos que verifica la propiedad reflexiva (apartado 1 de la proposición anterior) y la propiedad transitiva (apartado 2 de la proposición

anterior). En cambio no verifica la propiedad antisimétrica. Por tanto, ($\mathbb{Z}$,/) es un conjunto preordenado. Si un número entero y su opuesto fuesen el mismo se verificaría la propiedad antisimétrica y ($\mathbb{Z}$,/) sería un conjunto ordenado. Eso no es posible, pero vamos a evitar esa dificultad considerando equivalentes un número y su opuesto.

DEF Diremos que dos números enteros, a y b, son asociados si verifican a/b y b/a.

OBS Los números asociados se obtienen multiplicando por 1 y por –1.

Al conjunto formado por el 1 y –1 lo vamos a denotar por U={1,-1} y forman un grupo multiplicativo.

DEF Definimos la relación "ser asociados" y la denotaremos por $\cup$ a :

$$a \cup b \iff a/b \text{ y } b/a$$

PROP La relación $\cup$ es una relación de equivalencia.

Dem

Reflexiva: Dado $a \in \mathbb{Z}$ se verifica $a/a \Rightarrow a \cup a$

Simétrica: $a \cup b \Rightarrow a/b$ y $b/a \Rightarrow b/a$ y $a/b \Rightarrow b \cup a$

Transitiva: $a \cup b \Rightarrow a/b$ y b/a

$b \cup c \Rightarrow b/c$ y c/b

Como a/b y $b/c \Rightarrow a/c$ y como c/b y $b/a \Rightarrow c/a$

Entonces: $a \cup c$

La relación de equivalencia "ser asociados" define clases de equivalencia donde $\forall a \in \mathbb{Z}$ subclase de equivalencia la denotaremos $\bar{a}$ y $\mathbb{Z}/\cup$ es el conjunto cociente.

A los elementos del conjunto cociente (las clases de equivalencia) se les llama números asociados.

$$\bar{a} = \{b \in \mathbb{Z} / a \cdot u = b \text{ con } u \in U\}$$

Si: $a=0 \Rightarrow \bar{0} = \{0\}$

Si: $a \neq 0 \Rightarrow \bar{a} = \{a,-a\}$

Ya estamos en condiciones de generalizar la relación de divisibilidad definida en $\mathbb{Z}$ al conjunto $\mathbb{Z}/\cup$

DEF Dados $\bar{a}, \bar{b} \in \mathbb{Z}/\cup$, diremos que $\bar{a}$ divide a $\bar{b}$ si $\exists c \in \mathbb{Z}$ tal que $\bar{b} = \bar{a} \cdot c$

Con esta nueva relación de divisibilidad podemos afirmar:

PROP La relación de divisibilidad definida es una relación de orden y el conjunto $(\mathbb{Z}/\cup, /)$ es un conjunto ordenado.

OBS En la práctica, no hablamos de divisibilidad de números asociados, pero al tratar la propiedad antisimétrica, se considerarán las clases (o números asociados), no los números entre sí

PROP La divisibilidad entre números enteros verifica:

1) Si a/b y $a/c \Rightarrow a/b+c$ y $a/b-c$

2) Si $a/b \ \forall c\in\mathbb{Z} \Rightarrow a/b\cdot c$

Dem

1) $a/b \Rightarrow \exists n_1\in\mathbb{Z} / b=a\cdot n_1$

$a/c \Rightarrow \exists n_2\in\mathbb{Z} / c=a\cdot n_2$

$b+c=a\cdot n_1+a\cdot n_2 = a\cdot(n_1+n_2)$; Como $n_1+n_2\in\mathbb{Z} \Rightarrow a/b+c$

$b-c=a\cdot n_1-a\cdot n_2 = a\cdot(n_1-n_2)$; Como $n_1-n_2\in\mathbb{Z} \Rightarrow a/b-c$

2) $a/b \Rightarrow \exists n_1\in\mathbb{Z} / b=a\cdot n_1$

Al multiplicar ambos miembros por $c\in\mathbb{Z}$

$b\cdot c=(a\cdot n_1)\cdot c$; $b\cdot c=a\cdot(n_1\cdot c)$ y como $n_1\cdot c\in\mathbb{Z} \Rightarrow a/b\cdot c$

3.2. Divisibilidad en el Anillo de los Números Enteros.

DEF Sean $a,b\in\mathbb{Z}$. Diremos que "*a* divide a *b*" y se escribe a/b cuando $(b)\subset(a)$.

Ejemplo: $5/10$ ya que $(10)\subset(5)$

PROP Sean $a,b\in\mathbb{Z}$. Las definiciones vistas:

1) a/b si $\exists c\in\mathbb{Z} / b=a\cdot c$

2) a/b si $(b)\subset(a)$ son equivalentes

Dem

1) $\Rightarrow$ 2)

Si $a/b \Rightarrow \exists c\in\mathbb{Z} / b=a\cdot c \Rightarrow b\subset(a) \Rightarrow (b)\subset(a)$ por ser $\mathbb{Z}$ un anillo principal.

2) $\Rightarrow$ 1)

Si a/b $\Rightarrow$ (b)$\subset$(a) $\Rightarrow$ b$\in$(a) $\Rightarrow$ $\exists c\in\mathbb{Z}$ / b=a·c por ser $\mathbb{Z}$ un anillo principal.

PROP Dados a,b$\in\mathbb{Z}$, son asociados $\Leftrightarrow$ (a)=(b)

Dem

"$\Rightarrow$"

Como a y b son asociados $\Rightarrow$ a$\cup$b $\Rightarrow$ $\left.\begin{matrix} a/b \Rightarrow (b)\subset(a) \\ b/a \Rightarrow (a)\subset(b) \end{matrix}\right\}$ $\Rightarrow$ (b)=(a)

"$\Leftarrow$"

(a)=(b) $\Rightarrow$ $\left.\begin{matrix} (a)\subset(b) \Rightarrow b/a \\ (b)\subset(a) \Rightarrow a/b \end{matrix}\right\}$ $\Rightarrow$ a$\cup$b $\Rightarrow$ a y b son asociados.

OBS Un ideal en $\mathbb{Z}$ está engendrado por un elemento o por su opuesto (son los que pertenecen a la misma clase según la relación de equivalencia "ser asociado").

DEF Se dice que $\bar{a}$ divide a $\bar{b}$, y se escribe $\bar{a}/\bar{b}$ cuando (b)$\subset$(a)

PROP $\forall a,b\in\mathbb{N}$ con a/b se verifica:

1) a/b^n con $n\in\mathbb{N}$
2) a/|b|
3) |a|/|b|
4) b$\neq$0 $\Rightarrow$ |a|$\leq$|b|

Dem

1) Como a/b $\Rightarrow$ $\exists n_1\in\mathbb{N}$ / $b=a\cdot n_1$

n=1 trivial

n=k-1 supongamos cierto que a/b^{k-1}

n=k como a/b^{k-1} $\Rightarrow$ $\exists n_{k-1}\in\mathbb{N}$ / $b^{k-1}=a\cdot n_{k-1}$

$$b^k=b.b^{k-1}=a\cdot n_1\cdot a\cdot n_{k-1}$$

Sea: $n_k=a\cdot n_1\cdot n_{k-1}\in\mathbb{Z}$ $\quad$ $b^k=a\cdot n_k$ $\Rightarrow$ a/n^k

2) Si b$\geq$0 a/b por hipótesis

Si b<0 como a/b $\exists n_1 \in \mathbb{Z} / b=a\cdot n_1 \Rightarrow -b=a\cdot(-n_1) \Rightarrow a/-b$

entonces: $a/|b|$

3) y 4) Son análogas.

3.3. Máximo Común Divisor y Mínimo Común Múltiplo.

DEF Sean $a,b\in\mathbb{Z}$. Llamaremos "Máximo Común Divisor" de *a* y *b* a $d\in\mathbb{Z}$ verificando las siguientes condiciones:

1) d/a y d/b

2) $\exists s\in\mathbb{Z}$ / s/a y s/b $\Rightarrow$ s/d

OBS *d* es el mayor de los divisores comunes de *a* y *b*.

Podemos fácilmente extender la definición a un número de elementos de $\mathbb{Z}$.

DEF Sean $a_1, a_2, a_3,\ldots, a_n\in\mathbb{Z}$. Llamaremos M.C.D. de $a_1 \rightarrow a_n$ a $d\in\mathbb{Z}$ verificando:

1) $d/a_i \ \forall_i:1,\ldots,n$

2) $\exists s\in\mathbb{Z}$ / $s/a_i \ \forall_i:1,\ldots,n \Rightarrow s/d$

Diremos que $d=mcd(a_1 \rightarrow a_n)$

Las proposiciones que siguen vamos a demostrarlas para dos elementos, siendo su extensión a *n* elementos, inmediata.

PROP Sean $a,b\in\mathbb{Z}$. (a)+(b)=(d) si y sólo si d=mcd(a,b)

Dem

"$\Rightarrow$"

Hemos de probar que se verifican las siguientes condiciones de la definición:

1) Como (a)+(b)=(d) $\Rightarrow$ $a,b\in(d) \Rightarrow \begin{cases} a\in(d) \Rightarrow a=d\cdot n_1 \Rightarrow d/a \\ b\in(d) \Rightarrow b=d\cdot n_2 \Rightarrow d/b \end{cases}$

2) Supongamos que $\exists s\in\mathbb{Z}$ tal que s/a y s/b

$s/a \Rightarrow a=s\cdot m_1$

$s/b \Rightarrow b=s\cdot m_2$

como (a)+(b)=(d) $\Rightarrow d=a\cdot n_1+b\cdot n_2=s\cdot m_1\cdot n_1+s\cdot m_2\cdot n_2 \Rightarrow d=s(m_1\cdot n_1+\cdot m_2\cdot n_2) \Rightarrow s/d$

"$\Leftarrow$"

Como d=m.c.d(a,b) $\Rightarrow$ d/a y d/b $\Rightarrow$ $a\in(d)$ y $b\in(d)$ $\Rightarrow$ $(a)\subset(d)$ y $(b)\subset(d)$ $\Rightarrow$

$$\Rightarrow \quad (a)+(b)\subset(d)$$

Para ver la inclusión al contrario:

como la suma de ideales es un nuevo ideal y en $\mathbb{Z}$ los ideales son todos principales

$$\Rightarrow \quad \exists s\in\mathbb{Z} \,/\, (a)+(b)=(s)$$

pero entonces s/a y s/b

Por ser d=mcd(a,b) $\Rightarrow$ s/d $\Rightarrow$ $(d)\subset(s)=(a)+(b)$ por tanto $(d)=(a)+(b)$

OBS La proposición anterior demuestra la existencia de mcd de un número finito de elementos de $\mathbb{Z}$.

PROP Sean $a,b\in\mathbb{Z}$. Se verifica que el mcd(a,b) es único, salvo factores unidad de $\mathbb{Z}$.

Dem

Supongamos $\exists d,d'\in\mathbb{Z}$ / d=mcd(a,b) y d'=mcd(a,b)

De la proposición anterior $(a)+(b)=(d)=(d')$

Como $(d)=(d') \Rightarrow \begin{cases} d\in(d') \Rightarrow d=d_1\cdot d' \\ d'\in(d) \Rightarrow d'=d_2\cdot d \end{cases} \Rightarrow d=d_1\cdot d_2\cdot d$

Por ser $\mathbb{Z}$ un dominio de integridad $\Rightarrow$ $d_1\cdot d_2=1$ $\Rightarrow$ $d_1=d_2=1$ ó $d_1=d_2=-1$

Por tanto *d* y *d'* o son iguales o difieren en un factor unidad.

Por convenio, se toma como mcd el número positivo.

Teorema de BEZOUT.

Si d=mcd(a,b) entonces existen dos números $\lambda,\mu\in\mathbb{Z}$ tales que $d=\lambda a+\mu b$

Dem

d=mcd(a,b) $\Rightarrow$ (d)=(a)+(b) $\Rightarrow$ $\exists m,n\in\mathbb{Z}$ tal que d=m+n con $n\in(a)$ y $n\in(b)$

$\Rightarrow$ $m=a\cdot\lambda$ para algún $\lambda\in\mathbb{Z}$ y $n=b\cdot\mu$ para algún $\mu\in\mathbb{Z}$ $\Rightarrow$ $d=\lambda a+\mu b$

Algoritmo de la División

Sean $a,b\in\mathbb{Z}$ con b>0. Entonces existen $q,r\in\mathbb{Z}$ únicos tales que:

$$a=b\cdot q+r \quad \text{con} \quad 0\le r<b$$

Dem

Existencia Sean $a,b\in\mathbb{Z}$ con $b>0$

Construimos el conjunto $S=\{a-bn / n\in\mathbb{Z}$ y $a-bn$ es un número Natural$\}$

Es fácil comprobar que S no es vacío:

Si $a=0 \Rightarrow$ tomando $n=-1$ $a-b(-1)\geq 0$

Si $a\neq 0 \Rightarrow$ tomando $n=-a^2$ $a-b(-a^2)=a+b.a^2\geq 0$

Aplicando el principio de buena ordenación de $\mathbb{N}$, que dice que todo subconjunto de $\mathbb{N}$ no vacío, tiene un mínimo, existe $r=$mín S

Luego $r=a-b\cdot q$ para un determinado $q\in\mathbb{Z}$ y $r\geq 0$

Por tanto: $a=b\cdot q+r$ con $r\geq 0$.

Comprobemos ahora que $r<b$

$$\left.\begin{array}{l}\text{Supongamos que } r\geq b \Rightarrow a-bq-b=a-b(q+1)\\ r-b\geq 0\end{array}\right\} \Rightarrow r-b\in S$$

y $r-b<b$ ya que $b>0$

Pero sabemos que r=min S luego eso es imposible. Por tanto la suposición es falsa y $r<b$

Unicidad

Supongamos que existen $q,r,q',r'\in\mathbb{Z}$ tales que $a=b.q+r=b.q'+r'$ con $0\leq r<b$ y $0\leq r'<b$. Supongamos $r'\leq r$

$$\left.\begin{array}{l}\text{Entonces tenemos que: } b(q'-q)=r-r'\\ \text{pero como } r-r'<b\end{array}\right\} \Rightarrow q'-q=0$$

y si $q'-q=0 \Rightarrow r-r'=0$ y se obtiene que $q=q'$ y $r=r'$.

DEF Dados $a,b\in\mathbb{Z}$, diremos que a y b son coprimos (o sea, son primos entre sí) si mcd(a,b)=1.

PROP Si mcd(a,b)=d para $a,b\in\mathbb{Z}$ $\quad \text{mcd}\left(\frac{a}{d},\frac{b}{d}\right)=1$

Dem

Si mcd(a,b)=d $\Rightarrow$ d/a d/b

Por el Teorema de Bezout: $\exists \lambda,\mu \in \mathbb{Z} / d=\lambda a+\mu b \Rightarrow$

$$\Rightarrow 1 = \lambda \frac{a}{d} + m\frac{b}{d} \Rightarrow (1) \subset \left(\frac{a}{d}\right)+\left(\frac{b}{d}\right) \Rightarrow \left(\frac{a}{d}\right)+\left(\frac{b}{d}\right)=(1) \Rightarrow$$

$$\text{y como } (1)=\mathbb{Z} \Rightarrow \left(\frac{a}{d}\right)+\left(\frac{b}{d}\right) \subset (1)$$

$$\Rightarrow \text{mcd}\left(\frac{a}{d},\frac{b}{d}\right)=1$$

Teorema de EUCLIDES. Si $a/b\cdot c$ y $\text{mcd}(a,b)=1 \Rightarrow a/c$

Dem

Como mcd(a,b)=1. Por el teorema de Bezout $\exists \lambda,\mu \in \mathbb{Z} / 1=\lambda a+\mu b$

Al multiplicar la expresión por c $\Rightarrow$ $c=\lambda ac+\mu bc$

$$\left.\begin{array}{rl} a/a & \Rightarrow a/\lambda ac \\ \text{Por hipótesis} \quad a/bc & \Rightarrow a/mbc \end{array}\right\} \Rightarrow a/\lambda ac + mbc \Rightarrow a/c$$

DEF Sean $a,b \in \mathbb{Z}$. Llamaremos "Mínimo Común Múltiplo" de a y b a $m \in \mathbb{Z}$ si se verifican las siguientes condiciones:

1) a/m y b/m
2) $\exists n \in \mathbb{Z}$ tal que $a(n$ y $b/n \Rightarrow m/n$

OBS m es el menor de los múltiplos comunes de a y b.

Es inmediato extender la definición a un número *k* de elementos de $\mathbb{Z}$.

DEF Sean $a_1, a_2, a_3,.., a_k \in \mathbb{Z}$. Llamaremos mínimo común múltiplo de $a_1 \rightarrow a_k$ a $m \in \mathbb{Z}$ verificando las siguientes condiciones:

1) $a_i/m \ \forall_i:1,\ldots,k$
2) $\exists n \in \mathbb{Z}$ tal que $a_i/n \ \forall_i:1,\ldots,k \Rightarrow m/n$

Diremos que m=mcm(a,b)

Al igual que hemos hecho con el mcd, las proposiciones que siguen vamos a demostrarlas para dos elementos, siendo inmediato la extensión a *n* elementos.

PROP Sean $a,b \in \mathbb{Z}$. $(a)\cap(b)=(m)$ si y sólo si m=mcm(a,b)

Dem

"$\Rightarrow$" Hemos de probar que se verifican las dos condiciones de la definición:

1) Como $(a)\cap(b)=(m) \Rightarrow \begin{cases}(m)\subset(a) \Rightarrow m\in(a) \Rightarrow a/m\\ (m)\subset(b) \Rightarrow m\in(b) \Rightarrow b/m\end{cases}$

2) Supongamos que $\exists n\in\mathbb{Z}$ / a/n y b/n

$$\left.\begin{array}{l}\text{Como } a/n \Rightarrow n\in(a) \Rightarrow (n)\subset(a)\\ \text{Como } b/n \Rightarrow n\in(b) \Rightarrow (n)\subset(b)\end{array}\right\} \Rightarrow (n)\subset(a)\cap(b)=(m) \Rightarrow$$

$$\Rightarrow (n)\subset(m) \Rightarrow n\in(m) \Rightarrow m/n$$

"$\Leftarrow$" Como $m=mcm(a,b) \Rightarrow a/m$ y $b/m \Rightarrow m\in(a)$ y $m\in(b) \Rightarrow$

$$\Rightarrow (m)\subset(a)\cap(b)$$

Veamos la inclusión al revés.

Como la intersección de ideales es un nuevo ideal y en $\mathbb{Z}$ todos los ideales son principales, supongamos que $\exists t\in\mathbb{Z}$.

$$(a)\cap(b)=(t) \Rightarrow \begin{cases}(t)\subset(a) \Rightarrow t\in(a) \Rightarrow a/t\\ (t)\subset(b) \Rightarrow t\in(b) \Rightarrow b/t\end{cases}$$

Pero como $m=mcm(a,b)$ se verifica $m/t \Rightarrow (t)\subset(m)$

y como $(t)=(a)\cap(b)$ tenemos $(a)\cap(b)\subset(m)$

COROLARIO Dados $a,b\in\mathbb{Z}$, a/b si y sólo si $mcm(a,b)=b$

Dem

$a/b \Leftrightarrow (b)\subset(a) \Leftrightarrow (a)\cap(b)=(b) \Leftrightarrow mcm(a,b)=b$

PROP Si $mcm(a,b)=m \Rightarrow mcm(a\cdot c, b\cdot c)=m\cdot c$ con $c\neq 0$

Dem

Como $mcm(a,b)=m \Rightarrow (a)\cap(b)=(m) \Rightarrow (a.c)\cap(b.c)=(m.c) \Rightarrow$

$$\Rightarrow mcm(ac,bc)=mc$$

PROP Si $mcm(a,b)=m$ y $\exists c$ / c/a y c/b $\Rightarrow mcm\left(\frac{a}{c},\frac{b}{c}\right)=\frac{m}{c}$

Dem Análoga a la anterior.

Veamos ahora la relación que existe entre el mcd y el mcm de dos números enteros.

Teorema

Dados $a,b\in\mathbb{Z}$ $\text{mcd}(a,b)\cdot\text{mcm}(a,b)=a\cdot b$

Dem

Sea $\text{mcd}(a,b)=d$ y $\text{mcm}(a,b)=m$

Si $\text{mcd}(a,b)=d \Rightarrow \left.\begin{array}{l} d/a \Rightarrow a=a'.d \\ d/b \Rightarrow b=b'.d \end{array}\right\}$ verificando $\text{mcd}\left(\frac{a}{d},\frac{b}{d}\right)=1$

que es lo mismo que $\text{mcd}(a',b')=1$

Si $\begin{cases} a=a'd \Rightarrow a.b'=a'd.b' \Rightarrow a/a'd.b' \\ b=b'd \Rightarrow b.a'=b'd.a' \Rightarrow b/a'd.b' \end{cases}$

Sea k un múltiplo cualquiera de a y b. Entonces:

$\exists r,s\in\mathbb{Z}$ tales que $\begin{cases} k=a.r \Rightarrow k=a'd.r \\ k=b.s \Rightarrow k=b'd.s \end{cases} \Rightarrow a'd.r=b'd.s \Rightarrow a'r=b's \Rightarrow$

$\Rightarrow a'/b's$ y como $\text{mcd}(a',b')=1$, por el teorema de Euclides tenemos que:

$$a'/s \Rightarrow \exists t\in\mathbb{Z} \text{ tal que } s=a't$$

Por tanto $k=b.s=b.a't=b'd.a't \Rightarrow k/b'd.a'$

Podemos decir que $\text{mcm}(a,b)=d.a'b'$

Ya estamos en condiciones de comprobar la igualdad, que es $d.m=a.b$

$$d.m=d.d.a'b'=d.a'.d.b'=a.b \qquad \text{cqd}$$

COROLARIO $a,b\in\mathbb{Z}$ son coprimos $\Leftrightarrow$ $\text{mcm}(a,b)=a.b$

Dem

a,b son coprimos $\Leftrightarrow$ $\text{mcd}(a,b)=1$ $\Leftrightarrow$ $\text{mcm}(a,b)=a.b$

Vamos a ver ahora un teorema que nos va ha dar un método práctico para calcular el mcd de dos números y, aplicando el teorema anterior, podremos calcular a su vez, el mcm. Consiste en las divisiones sucesivas.

Teorema del Algoritmo de EUCLIDES.

Si r es el resto de la división entera de *a* por *b*, entonces $\text{mcd}(a,b)=\text{mcd}(b,r)$

Dem Dados $a,b\in\mathbb{Z}$ $\exists q,r\in\mathbb{Z}$ / $a=b.q+r$ $0\le r<b$

$r=a-b.q=a.1+b.(-q)$ luego todo divisor de *a* y *b* es también divisor de *r*.

$r\in(a)+(b) \Rightarrow r\in(d)$ siendo $d=mcd(a,b) \Rightarrow (r)\subset(d) \Rightarrow d/r \Rightarrow$

$\Rightarrow mcd(b,r)=d=mcd(a,b)$

Llamaremos Algoritmo de Euclides al proceso de divisiones sucesivas que nos va a permitir calcular el mcd de dos números.

Algoritmo de Euclides: Dados $a,b\in\mathbb{Z}$

$\exists q_1,r_1 \quad a=bq_1+r_1 \quad 0\le r_1<b \Rightarrow mcd(a,b)=mcd(b,r_1)$

Si $r_1=0 \Rightarrow mcd(b,0)=b$ y se para. En caso contrario se repite para b,r_1

$\exists q_2,r_2 \quad b=r_1q_2+r_2 \quad 0\le r_2<r_1 \Rightarrow mcd(b,r_1)=mcd(r_1,r_2)$

Si $r_2=0 \Rightarrow mcd(r_1,0)=r_1$. En caso contrario se repite

Después de *n* pasos llegaremos a que:

$r_{n-2}=r_{n-1}.q_n+r_n$ con $r_n=0 \Rightarrow mcd(a,b)=mcd(b,r_1)=\ldots=mcd(r_{n-1},0)=r_{n-1}$

4. NÚMEROS PRIMOS.

DEF Sea $p\in\mathbb{Z}-\{0,1,-1\}$. Diremos que p es un número primo si sólo es divisible por unidades y por sus asociados.

OBS p es primo si sus únicos divisores son {-1, 1, p, -p}

DEF Sea $q\in\mathbb{Z}-\{0,1,-1\}$. Diremos que q es compuesto si no es un número primo.

OBS Los números $-1,0,1\in\mathbb{Z}$ no son números primos ni son números compuestos.

Veamos algunas propiedades de los Números Primos.

PROP Sea $p\in\mathbb{Z}$ un número primo. Si $p/a \Rightarrow mcd(p,a)=p$

Dem

Vamos a suponer que $p>0$ ya que no afecta.

Sea $mcd(a,p)=d \Rightarrow$ d es el mayor de los divisores comunes a *a* y *p*.

$d/a \Rightarrow$ por ser p primo $d\in\{1,-1,p,-p\}$

Como p/a tenemos que todos los divisores de p son divisores de a. Luego todos los divisores de p y de a son $\{-1,1,-p,p\}$.

Como d es el mayor de todos, entonces d=p. Por tanto mcd(a,p)=p

PROP Sea $p \in \mathbb{Z}$ un número primo. Si $p/a.b \Rightarrow p/a$ ó p/b

Dem

Si p/a entonces la proposición ya está demostrada.

Supongamos que *p* no divide a *a*, entonces mcd(p,a)=1.

Aplicando el Teorema de Euclides: p/a.b y mcd(p,a) $\Rightarrow$ p/b

PROP El conjunto de los números primos es infinito.

Dem

Supongamos que el conjunto de los números primo es finito

Sea $P=\{p_1,p_2,\ldots,p_n\}$ todos los números primos.

Sea $q=p_1 \cdot p_2 \cdot \ldots \cdot p_n+1$. Vamos a comprobar que q es primo, lo que supondrá una contradicción, ya que $q \notin P$

Si q no es primo $\Rightarrow$ $\exists i \in \{1,\ldots n\}$ / p_i/q $\Rightarrow$ $\exists c \in \mathbb{Z}$ / $q=p_i \cdot c$

Entonces: $p_i \cdot c=p_1 \cdot p_2 \cdot \ldots \cdot p_n+1$ $\Rightarrow$

$$\Rightarrow \quad c=\frac{p_1 \cdot p_2 \cdot \ldots \cdot p_n}{p_i}+\frac{1}{p_i}= p_1 \cdot \ldots \cdot p_{i-1} \cdot p_{i+1} \cdot \ldots \cdot p_n+\frac{1}{p_i} \quad \Rightarrow$$

$$\Rightarrow \quad \frac{1}{p_i}=c-p_1 \cdot \ldots \cdot p_{i-1} \cdot p_{i+1} \cdot \ldots \cdot p_n \in \mathbb{Z}$$

$\Rightarrow$ $p_i/1$ con p_i primo, lo que es una contradicción $\Rightarrow$ q es primo $\Rightarrow$

$\Rightarrow$ El conjunto de los números primos es infinito

Para poder obtener todos los números primos inferiores a uno dado existe un método práctico que recibe el nombre de Criba de Erastótenes.

Criba de Erastótenes.

Se escribe la sucesión de los números naturales hasta el número dado. A continuación tachamos todos los múltiplos de 2 comenzando en su cuadrado $2^2=4$. A continuación del 2, el primer número sin tachar es el 3, entonces eliminamos los múltiplos de 3 comenzando en su cuadrado $3^2=9$. Repetimos el proceso hasta llegar a un número cuyo cuadrado no esté en la lista. Aquellos números que permanezcan sin tachar son números primos.

Dado un número entero, para comprobar si es número primo sin tener que realizar la criba de Erastótenes, basta con comprobar si es divisible por los primeros números primos (2,3,5,7,…) hasta que se llegue a un número cuadrado sea superior al propio número dado.

Teorema En $\mathbb{Z}$ se verifica: p es primo $\Leftrightarrow$ (p) es ideal maximal

Dem

"$\Rightarrow$"

Como p es primo $\Rightarrow$ $(p)\neq\mathbb{Z}$ ya que $p\neq\pm1$

Sea (q) un ideal tal que $(p)\subset(q)\subset\mathbb{Z}$.

Como $(p)\subset(q)$ $\Rightarrow$ q/p pero al ser p primo $q\in\{1,-1,p,-p\}$

Sea $u\in\{-1,1\}$ $\Rightarrow$ $\begin{cases} q=u \Rightarrow (q)=(u)=\mathbb{Z} \\ q=u\cdot p \Rightarrow (p)=(q) \end{cases}$

Entonces (p) es ideal maximal al verificar las dos condiciones de la definición.

"$\Leftarrow$"

Sea q un divisor de p $\Rightarrow$ q/p $\Rightarrow$ $(p)\subset(q)$

Como (p) es maximal $\Rightarrow$ Si $(p)\subset(q)$ se verifica que (q)=(p) ó $(q)=\mathbb{Z}$

Si (q)=(p) $\Rightarrow$ p/q y q/p $\Rightarrow$ p y q son asociados $\Rightarrow$ p es sólo divisible por sus asociados.

Si $(q)=\mathbb{Z}$ $\Rightarrow$ q=u $\Rightarrow$ $(p)\subset(u)$ $\Rightarrow$ u/p entonces p es sólo divisible por las unidades o por sus asociados $\Rightarrow$ p es primo

DEF Se llaman números primarios a las potencias de la forma p^n siendo p un número primo y $n\in\mathbb{N}-\{0\}$

OBS Todo número primo es número primario, sin más que tomar n=1.

Ahora vamos a ver un resultado que nos va a permitir decir que todo número compuesto admite una descomposición en factores primarios y que dos descomposiciones del mismo número son iguales salvo en el signo de los factores.

Si traducimos esto a ideales, es lo mismo que decir que todo ideal propio de $\mathbb{Z}$ admite una descomposición como intersección finita de ideales primarios.

Por ejemplo: $(50)=(2)\cap(5^2)$ siendo (2) y (5^2) ideales primarios.

Teorema Fundamental de la Aritmética.

a) Existencia: Todo número compuesto se puede descomponer en un producto de factores primos.

b) Unicidad: La descomposición anterior es única, salvo el orden o signo de los factores.

Dem

a) Existencia.

Sea m un número compuesto y p el divisor primo de m, más pequeño.

Entonces $m=p_1.n_1$ con $n_1 \in \mathbb{Z}$

Si n_1 es primo, ya está demostrado. m sería el producto de dos primos

Si n_1 no es primo, repetimos el proceso para n_1.

Sea p_2 el divisor primo de n_1 más pequeño:

Entonces $n_1=p_2.n_2$ con $n_2 \in \mathbb{Z}$ luego $m=p_1.p_2.n_2$

Repetimos el proceso hasta obtener $n_k \in \mathbb{Z}$ número primo para algún k o es una unidad.

El proceso es finito, ya que, por ejemplo, si usáramos el método de la Criba de Erastótenes, obtendríamos un número finito de números primos, que son los candidatos a ser divisores de m (los números primos mayores que m no pueden dividirlo)

Si n_k es una unidad $\Rightarrow$ $m=p_1.p_2.p_3\ldots.p_k$

Si n_k es número primo $\Rightarrow$ $p_{k+1}=n_k$ y $m= p_1.p_2.p_3\ldots.p_k.p_{k+1}$.

b) Unicidad.

Una vez comprobado que m se puede descomponer como producto de números primos, veamos que dicha descomposición es única.

Sea $m= p_1.p_2.p_3\ldots.p_n=q_1.q_2.q_3\ldots.q_k$. $n<k$

Para ver que la descomposición es única debemos demostrar que:

i) $n=k$
ii) $p_i=q_i.u_i$ para $i=1,\ldots,n$ y $u_i \in \{1,-1\}$ unidades de $\mathbb{Z}$.

Como $p_1...p_n=q_1\ldots q_k$ $\Rightarrow$ $p_1/q_1\ldots q_k$ y como p_1 es primo $\Rightarrow$

$\Rightarrow$ $\exists j \in \{1,\ldots,k\}$ / p_1/q_j y como q_j también es primo $\Rightarrow$

$\Rightarrow$ p_1 y q_j son asociados $\Rightarrow$ $p_1=q_j.u$ con $u \in \{-1,1\}$.

Reordenando los números primos podemos afirmar que $p_1=q_1.u_1$

Entonces: $p_1.(p_2\ldots p_n)=q_1.(q_2\ldots q_k)$ se transforma en:

$q_1.u_1.(p_2\ldots p_n)=q_1.(q_2\ldots q_k)$ quedando: $u_1.p_2\ldots p_n=q_2\ldots q_k$

Repitiendo todo este proceso n veces obtenemos:

$$u_1.u_2\ldots u_n=q_{n+1}\ldots q_k$$

Luego: $q_{n+1}\ldots q_k=1$ ó $q_{n+1}\ldots q_k=-1$

Entonces $\forall j \in \{n+1,\ldots,k\}$ tenemos $q_j/1$ ó $q_j/-1$

Por tanto: $q_j=u$ con $u \in \{1,-1\}$ y $j \in \{n+1,\ldots,k\}$

Obtenemos que $m=p_1\ldots p_n=q_1\ldots q_n$ y $p_i=q_i.u_i$ $\forall i:1\ldots n$ c.q.d.

COROLARIO

Si en la descomposición de un número compuesto aparecen varios números primos repetidos, se pueden asociar y el número se escribe así:

$m = p_1^{a_1}.p_2^{a_2}....p_n^{a_n}$ siendo a_i el número de veces que se repite p_i i:1,…,n

Dem

Dado $m \in \mathbb{Z}$ número compuesto, como la descomposición es única, si ordenamos los números primos de menor a mayor, tenemos:

$$m = p_1..\overset{a_1}{\ldots}..p_1.p_2..\overset{a_2}{\ldots}..p_2.....p_n..\overset{a_n}{\ldots}..p_n = p_1^{a_1}.p_2^{a_2}.....p_n^{a_n}$$

COROLARIO

Todo número compuesto se puede descomponer de manera única como producto de números primos.

Dem

Igual que la demostración anterior.

COROLARIO

Todo ideal propio de $\mathbb{Z}$ se puede poner como intersección finita de ideales primarios

Dem

Dado $m \in \mathbb{Z}$ y aplicando el corolario anterior: $m = p_1^{a_1}.p_2^{a_2}.....p_n^{a_n}$

Es evidente que $mcd(p_1^{a_1}.p_2^{a_2}.....p_n^{a_n}) = 1$

ya que los p_i son todos distintos: $p_i \neq p_j \quad i \neq j$.

Entonces, como $mcd(p_1^{a_1}.p_2^{a_2}.....p_n^{a_n}) \cdot mcm(p_1^{a_1}.p_2^{a_2}.....p_n^{a_n}) = p_1^{a_1}.p_2^{a_2}.....p_n^{a_n}$

tenemos que: $mcm(p_1^{a_1}.p_2^{a_2}.....p_n^{a_n}) = m$

Por un teorema anterior comprobamos que $mcm(a,b)=m \Leftrightarrow (m)=(a)\cap(b)$

y aplicándolo obtenemos: $(m)=\left(p_1^{a_1}\right)\cap\left(p_2^{a_2}\right)\cap.....\cap\left(p_n^{a_n}\right)$ c.q.d.

Una consecuencia práctica de todo esto es la siguiente:

Dado $a,b \in \mathbb{Z}$ sabemos que mcd(a,b)=d es el mayor de los divisores comunes de a y b; mcm(a,b)=m es el menor de los múltiplos comunes distintos de cero de a y b.

Entonces el mcd(a,b)=d se puede obtener multiplicando los factores primos comunes con el menor exponente, de los que aparecen al descomponer a y b.

A su vez, el mcm(a,b)=m se puede obtener multiplicando los factores comunes y no comunes con el mayor exponente de los que aparecen en las descomposiciones de a y b.

5. CONGRUENCIAS.

DEF Sean $a,b,n \in \mathbb{Z}$ con n>0. Diremos que *a* es congruente con *b* módulo *n*, y se escribe $a \equiv b \pmod n$ si *n* divide a *a-b*, n/a-b, o lo que es lo mismo $a-b \in (n)$

PROP Sean $a,b,n \in \mathbb{Z}$ con n>0.

$a \equiv b \pmod n \Leftrightarrow$ a y b dan el mismo resto al dividirlos por n.

Dem

"$\Rightarrow$"

Sea $a \equiv b \pmod n \Leftrightarrow n/a-b \Rightarrow \exists c \in \mathbb{Z} / a-b=n.c$

Si dividimos b por n $\exists q,r \in a \equiv b \pmod n / b=n.q+r$ con $0 \leq r < n$

Hemos de comprobar que al dividir a por n también nos da de resto r.

Como $a-b=n.c \Rightarrow a=n.c+b \Rightarrow a=n.c+n.q+r \Rightarrow a=n.(c+q)+r$ con $0 \leq r < n$ cqd

"$\Leftarrow$"

Para ver que $a \equiv b \pmod n$ basta comprobar que $a-b \in (n)$

Por hipótesis $\exists q_1, r \in \mathbb{Z} / a = q_1.n + r \quad 0 \le r < n$

$\exists q_2 \in \mathbb{Z} / b = q_2.n + r$

Si restamos ambas expresiones: $a-b = n(q_1-q_2) \Rightarrow a-b \in (n)$ c.q.d.

PROP La relación de congruencia módulo n, es una relación de equivalencia que tienen exactamente n clases.

Dem

Usando el resultado de la proposición anterior, es trivial comprobar que la relación de congruencia verifica las propiedades reflexiva, simétrica y transitiva.

Reflexiva: $a \equiv a \pmod n$ ya que ambos (el propio a) tiene el mismo resto al ser divididos por n

Simétrica: Si a y b tienen el mismo resto, también b y a.

$$a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$$

Transitiva: Si a y b tienen el mismo resto y b y c también, entonces es claro que a y c lo van a tener.

$$a \equiv b \pmod n \quad y \quad b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$$

Veamos que tiene exactamente n clases.

Sea $a \in \mathbb{Z}$ arbitrario y $n>0$. Por el algoritmo de la división:

$$\exists q, r \in \mathbb{Z} / a = n.q + r \quad con \quad 0 \le r < n$$

$$a = n.q + r \Rightarrow a - r = n.q \Rightarrow n/a - r \Rightarrow a \equiv r \pmod r \Rightarrow [a] = [r]$$

y como $r \in \{0,1,\ldots,n-1\} \Rightarrow [a]$ coincide con alguna de las clases $\{[0],[1],\ldots[n-1]\}$ y son exactamente *n*, ya que son todos los valores que puede tomar *r*.

PROP Sean $a,b,a',b' \in \mathbb{Z}$ con $n>0$. Si

$$\left.\begin{array}{l} a \equiv a' \pmod n \\ b \equiv b' \pmod n \end{array}\right\} \Rightarrow \begin{cases} i) & a+b \equiv a'+b' \pmod n \\ ii) & a \cdot b \equiv a' \cdot b' \pmod n \end{cases}$$

Dem

i) $$\left.\begin{array}{l} a \equiv a' \pmod n \\ b \equiv b' \pmod n \end{array}\right\} \Rightarrow \begin{cases} n/a - a' \\ n/b - b' \end{cases} \Rightarrow n/(a-a') + (b-b') \Rightarrow$$

$$\Rightarrow n/(a+b) - (a'+b') \Rightarrow a+b \equiv a+b' \pmod n$$

ii) $\left.\begin{array}{l} a \equiv a'(\text{mod } n) \\ b \equiv b'(\text{mod } n) \end{array}\right\} \Rightarrow \begin{cases} n/a - a' \\ n/b - b' \end{cases} \Rightarrow \begin{cases} n/b.(a - a') \\ n/a.(b - b') \end{cases} \Rightarrow n/b(a - a') + a'(b - b') \Rightarrow$

$\Rightarrow \quad n/ab - a'b' \quad \Rightarrow \quad ab \equiv a'b'(\text{mod } n)$

COROLARIO

Sean $a,b,c,n \in \mathbb{Z}$ con $n>0$. Se verifica:

1) $a \equiv b(\text{mod } n) \Leftrightarrow \forall c \in \mathbb{Z} \quad a+c \equiv b+c \ (\text{mod } n)$

2) $a \equiv b(\text{mod } n) \Rightarrow \forall c \in \mathbb{Z} \quad a \cdot c \equiv b \cdot c \ (\text{mod } n)$

Dem

1) "⇒"

$\forall c \in \mathbb{Z}$ se verifica $n/c-c$ ya que $c-c=n.0 \Rightarrow c \equiv c(\text{mod } n)$

Aplicando i) de la proposición anterior a

$$\left.\begin{array}{r} a + c \equiv b + c(\text{mod } n) \\ c \equiv c(\text{mod } n) \end{array}\right\} \Rightarrow a+c \equiv b+c(\text{mod } n) \quad \forall c \in \mathbb{Z}$$

"⇐"

Análogamente podemos obtener que $\forall c \in \mathbb{Z} \quad -c \equiv -c(\text{mod } n)$

Aplicando i) de la proposición anterior a

$$\left.\begin{array}{r} a + c \equiv b + c(\text{mod } n) \\ -c \equiv -c(\text{mod } n) \end{array}\right\} \Rightarrow a \equiv b(\text{mod } n)$$

2) $\forall c \in \mathbb{Z} \quad c \equiv c(\text{mod } n)$

Aplicando ii) de la proposición anterior a:

$$\left.\begin{array}{l} a \equiv b(\text{mod } n) \\ c \equiv c(\text{mod } n) \end{array}\right\} \Rightarrow a.c \equiv b.c(\text{mod } n)$$

OBS El recíproco de 2) no se puede obtener si no añadimos alguna condición adicional. Veámoslo:

Sean $a,b,c,n \in \mathbb{Z}$ con $n>0$. Se verifica:

$ac=bc(\text{mod } n)$ y c y n son coprimos $\Rightarrow$ $a \equiv b(\text{mod } n)$

Dem

c y n son coprimos $\Leftrightarrow$ mcd(c,n)=1 $\Leftrightarrow$

aplicando el teorema de Bezaut

$\Leftrightarrow$ $\exists\lambda,\mu\in\mathbb{Z}$ / $1=\lambda.c+\mu.n$ $\quad 1+\lambda c=\mu n \Leftrightarrow n/1-\lambda.c \Leftrightarrow 1\equiv\lambda c(\text{mod } n)$

Como $a,b\in\mathbb{Z}$, se verifica $\begin{cases} a\equiv a(\text{mod } n) \\ b\equiv b(\text{mod } n) \end{cases}$

De $1\equiv\lambda c(\text{mod } n)$ y $a\equiv a(\text{mod } n)$ obtenemos $a\equiv\lambda ca(\text{mod } n)$

De $1\equiv\lambda c(\text{mod } n)$ y $b\equiv b(\text{mod } n)$ obtenemos $b\equiv\lambda cb(\text{mod } n)$

$$\left.\begin{array}{l} \text{Por hipótesis} \quad a.c\equiv b.c(\text{mod } n) \\ \text{como } l\in Z \quad l\equiv l(\text{mod } n) \end{array}\right\} \Rightarrow \lambda ac\equiv\lambda bc(\text{mod } n)$$

Aplicando la propiedad transitiva que verifica la relación de congruencia:

$$\left.\begin{array}{l} a\equiv lca(\text{mod } n) \\ b\equiv lcb(\text{mod } n) \\ lca\cong lcb(\text{mod } n) \end{array}\right\} \Rightarrow a\equiv b(\text{mod } n)$$

PROP Sean $a,b,k,n\in\mathbb{Z}$ con n>0.

$$\left.\begin{array}{l} a\equiv b \bmod (kn) \\ k\neq 0 \end{array}\right\} \Rightarrow a\equiv b(\text{mod } n)$$

Dem

$a\equiv b(\text{mod } kn) \Leftrightarrow kn/a-b \Rightarrow \exists c\in\mathbb{Z}$ / $a-b=ckn \Rightarrow a-b=(c.k).n \Rightarrow$

$\Rightarrow n/a-b \Rightarrow a\equiv b(\text{mod } n)$

Análogamente $a\equiv b(\text{mod } k)$

6. CRITERIOS DE DIVISIBILIDAD.

Antes de poder tratar los criterios de divisibilidad, hemos de obtener unos resultados previos,

DEF Sea p un número entero estrictamente positivo. Llamaremos restos potenciales de p, módulo n a los deferentes restos que se obtienen al dividir las sucesivas potencias de p por n.

Por ejemplo: Sea p=3 y n=10

$$3^0 \equiv 1 \pmod{10}$$
$$3^1 \equiv 3 \pmod{10}$$
$$3^2 \equiv 9 \pmod{10}$$
$$3^4 \equiv 7 \pmod{10}$$

A partir de esta definición podemos obtener las siguientes consecuencias:

1) El primero de los restos r_0 es siempre $r_0=1$

   Dados p y n, siempre se verifica que $p^0 \equiv 1 \pmod{10}$

2) El número de posibles restos potenciales distintos es finito, pues tienen que ser menores que n.

3) Si llamamos r_k al resto potencial que se obtiene al dividir p^k por n, entonces:

$$p^k \equiv r_k \pmod{n}$$

   Se verifica que $p^{k+1} \equiv r_k \pmod{n}$ lo que nos da un método recurrente de hallar un resto a partir del anterior.

$$r_k . p \equiv r_{k+1} \pmod{n}$$

   Es evidente que si algún resto es nulo, lo serán todos los siguientes.

PROP Sea $m=a_0p^0+ a_1p^1+\ldots+a_kp^k$ un número entero escrito en base p.

Si $r_0, r_1,\ldots,r_k$ son los restos potenciales de p modulo n, entonces:

$$m \equiv a_0r_0+a_1r_1+\ldots+a_kr_k \pmod{n}$$

Dem

$$p^i \equiv r_i \pmod{n} \quad \forall_i:0,\ldots,k \quad \Rightarrow \quad a_i.p^i \equiv a_ir_i \pmod{n} \quad \forall_i:0,\ldots,k$$

Al sumar las k+1 congruencias:

$$a_0p^0+ a_1p^1+\ldots+a_kp^k \equiv a_0r_0+a_1r_1+\ldots+a_kr_k \pmod{n}$$

lo que es lo mismo que:

$$m \equiv a_0r_0+a_1r_1+\ldots+a_kr_k \pmod{n}$$

COROLARIO m es divisible por n si y sólo si $a_0r_0+a_1r_1+\ldots+a_kr_k$ es divisible por n.

Dem

"$\Rightarrow$"

$$\left.\begin{array}{l} \text{m es divisible por n} \Leftrightarrow m \equiv 0 \pmod{n} \\ \text{como} \quad m \equiv a_0 r_0 + \ldots + a_k r_k \pmod{n} \end{array}\right\} \Rightarrow$$

Aplicando la propiedad transitiva:

$$\Rightarrow \quad a_0r_0+\ldots+a_kr_k \pmod n \quad \Rightarrow \quad a_0r_0+\ldots+a_kr_k \text{ es divisible por n}$$

"$\Leftarrow$"

Demostración análoga.

Vamos a aplicar todo lo visto al sistema decimal, es decir: p=10

En la tabla siguiente aparecen los restos potenciales de 10 respecto de los módulos 2,3,4,5,8,9 y 11.

$n\backslash r_i$	r_0	r_1	r_2	r_3	r_4	r_5	r_6
2	1	0	0	0	0	0	0
3	1	1	1	1	1	1	1
4	1	2	0	0	0	0	0
5	1	0	0	0	0	0	0
8	1	2	4	0	0	0	0
9	1	1	1	1	1	1	1
11	1	10	1	10	1	10	1

Al expresar m en base 10 tenemos:

$$m=a_0+a_1.10+a_2.100+\ldots.+a_k.10^k$$

siendo a_0 las unidades, a_1 las decenas, a_2 las centenas y así sucesivamente.

a) Criterio de divisibilidad por 2.

Como $m\equiv a_0 \pmod 2$, para que m sea divisible por 2 basta con que a_0 sea múltiplo de 2. Es decir, las unidades de m ha de ser un número múltiplo de 2.

b) Criterio de divisibilidad por 3.

Como $m\equiv a_0+a_1+\ldots+a_k \pmod 3$, la suma de todas las cifras de m ha de ser múltiplo de 3.

c) Criterio de divisibilidad por 4.

Como $m\equiv a_0+2a_1 \pmod 4$, la suma de las unidades mas el doble de las decenas ha de ser múltiplo de 4

d) Criterio de divisibilidad por 5.

Como $m\equiv a_0 \pmod 5$, la cifra de las unidades ha de ser múltiplo de 5, es decir ha de ser 0 ó 5.

e) Criterio de divisibilidad por 8.

Como $m=a_0+2a_1+4a_2 \pmod 8$, la suma de la cifra de las unidades mas el doble de las decenas mas el cuádruple de las centenas ha de ser múltiplo de 8

f) Criterio de divisibilidad por 9.

Como $m \equiv a_0+a_1+\ldots+a_k \pmod 9$, la suma de todas las cifras de m ha de ser un múltiplo de 9

g) Criterio de divisibilidad por 11.

Como $m=a_0+10a_1+a_2+10a_3+\ldots. \pmod{11}$ y teniendo en cuenta que: $10 \equiv -1 \pmod{11}$ quedaría

$$m=a_0-a_1+a_2-a_3+\ldots.+(-1)^k a_k \pmod{11}$$

Por tanto, un número m es divisible por 11 si la suma de sus cifras que ocupan lugar impar menos la suma de las cifras que ocupan lugar par, es un múltiplo de 11.

BIBLIOGRAFÍA RECOMENDADA.

Análisis Matemático I. Aut. J.A. Fernández Viña. Ed. Tecnos

Curso de Álgebra y Geometría. Aut. Juan de Burgos. Ed. Alhambra.

Algebra Moderna. Aut. A. Lentín, J. Rivaud, Ed. Aguilar.