Los números enteros.

Si m y n son números naturales y m<n, entonces existe r en **N** tal que m+r=n, y podemos definir la *resta* n-m como r. Para poder definir la resta n-m cuando m≥n necesitamos mas números.

Los números *enteros* se obtienen de los naturales agregando el 0 y añadiendo para cada natural n, otro número -n:

$$\mathbf{Z}=\{...,-3,-2,-1,0,1,2,3,...\}$$

La suma en **N** se extiende a todo **Z** definiendo:

- $0+0=0$,
- $n+0=0+n=n$
- $(-n)+0=0+(-n)=-n$
- $n+(-n)=(-n)+n=0$
- $(-m)+(-n)=-(m+n)$
- $m+(-n)=(-n)+m=\begin{cases} m-n & \text{si } m>n \\ -(n-m) & \text{si } n>m \end{cases}$

La multiplicación en **N** se extiende a **Z** definiendo:

- $0\cdot 0=0$
- $0\cdot n=n\cdot 0=0$
- $m\cdot(-n)=(-m)\cdot n= -m\cdot n$
- $(-m)\cdot(-n)=m\cdot n$

La suma y el producto definidos en **Z** cumplen las siguientes propiedades:

1. $r+s = s+r$ — *la suma es conmutativa*
2. $r+(s+t) = (r+s)+t$ — *la suma es asociativa*
3. $0+r = r+0 = r$ — *existe un neutro aditivo*
4. $r+(-r) = (-r)+r = 0$ — *hay inversos aditivos*

5. $r\cdot s = s\cdot r$ — *la multiplicación es conmutativa*
6. $r\cdot(s\cdot t) = (r\cdot s)\cdot t$ — *la multiplicación es asociativa*
7. $1\cdot r = r\cdot 1 = r$ — *existe un neutro multiplicativo*

8. $r\cdot(s+t) = r\cdot s+r\cdot t$, $(s+t)\cdot r = s\cdot r+t\cdot r$ — *la multiplicación se distribuye con la suma*

Z es el primer ejemplo de un **anillo**, que se un conjunto de "números" con dos operaciones que denotaremos como + y ▪ que cumplan las propiedades 1,2,3,4,6 y 8 (pero pueden ser muy distintas a la suma y al producto de enteros). Los anillos que ademas cumplen la propiedad 5 se llaman **anillos conmutativos** y si cumplen la propiedad 7 se llaman **anillos con unidad**.

Existen muchos anillos distintos, unos tienen muy pocos elementos y otros tienen muchísimos.

Ejemplo. El anillo mas chico tiene solo 2 elementos: 0 y 1, que se suman y se multiplican así:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Se puede mostrar que estas 2 operaciones tienen todas las propiedades 1 a 8, así que este anillo, conocido como $\mathbf{Z}_2$, es un anillo conmutativo con unidad.

Otros anillos están formados por polinomios, o por matrices, o por funciones. Mas adelante veremos que existen muchísimos anillos mas.

La suma y la multiplicación en **Z** tienen otras propiedades:

- $0 \cdot r = r \cdot 0 = 0$
- Si $r \cdot s = 0$ entonces $r=0$ o $s=0$ *no hay divisores de 0*

- Si $r+t = s+t$ entonces $r=s$ *ley de cancelación para la suma*
- Si $r \cdot s = r \cdot t$ y $r \neq 0$ entonces $s=t$ *ley de cancelación para el producto*

Uno puede preguntarse si estas ultimas propiedades son especiales de **Z** o si se cumplen en todos los anillos.

- ¿Será cierto que en todos los anillos $0 \cdot r = r \cdot 0 = 0$?

  Esto es cierto si podemos demostrarlo usando solo las propiedades de los anillos.

  $0 \cdot r = (0+0) \cdot r$ *ya que* $0+0=0$
  $0 \cdot r = 0 \cdot r + 0 \cdot r$ *distributividad*
  $0 \cdot r + (-0 \cdot r) = (0 \cdot r + 0 \cdot r) + (-0 \cdot r)$ *sumando* $-0 \cdot r$ *a cada lado*
  $0 \cdot r + (-0 \cdot r) = 0 \cdot r + (0 \cdot r + (-0 \cdot r))$ *asociatividad de la suma*
  $0 = 0 \cdot r + 0$ *0 es neutro aditivo*
  $0 = 0 \cdot r$

- ¿Será cierto que en todos los anillos $r+t = s+t \Rightarrow r = s$?

  Esto vale en todos los anillos, pues sale de las propiedades 2,3 y 4:

  $r+t = s+t$
  $(r+t)+(-t) = (s+t)+(-t)$ *existen inversos aditivos*
  $r+(t-t) = s+(t-t)$ *asociatividad de la suma*
  $r+0 = s+0$ *0 es neutro aditivo*
  $r = s$.

- ¿Será cierto que en todos los anillos $r \cdot s = 0 \Rightarrow r=0$ o $s=0$?

  Esto equivale a pedir que el producto de dos números distintos de 0 sea distinto de 0.
  Pero esto no se puede demostrar a partir de las propiedades de los anillos: existen anillos donde no se cierto.

- ¿Será cierto que en todos los anillos $r\cdot s = r\cdot t$ y $r\neq 0 \Rightarrow s=t$?
  Esto NO vale en todos los anillos. Veamos a que llegamos si tratamos de demostrarlo usando las propiedades:
  $r\cdot s = r\cdot t$
  $r\cdot s - r\cdot t = 0$ *sumando el inverso de* $r\cdot t$
  $r\cdot (s-t) = 0$ *distributividad*
  $s - t = 0$ *ya que* $r\neq 0$?
  $s = t$
  .

  Esto sería cierto si supiéramos que el producto de dos números distintos de 0 es distinto de 0, pero esto no ocurre en todos los anillos.

Los anillos donde se cumple la propiedad

9. Si $r\cdot s=0$ entonces $r=0$ o $s=0$ *no hay divisores de 0*

se llaman **dominios enteros**. En estos anillos si se cumple la ley de cancelación del producto. Ya veremos que hay muchos dominios enteros además de **Z**.

Problemas.

1. Muestra que los enteros pares forman un anillo con la suma y el producto usuales, pero los enteros impares no.

2. Demuestra que en todos los anillos se cumple que $a\cdot(-b)=(-a)\cdot b=-(a\cdot b)$

3. En los anillos podemos definir la resta usando la suma y los inversos aditivos: $a-b = a+(-b)$
   Pero la suma y la resta tienen propiedades muy distintas.
   a. La resta no es conmutativa... ¿o habrán anillos donde si lo sea?
   b. ¿La resta es asociativa?
   c. ¿El producto se distribuye con la resta?

4. Podemos construir unos números raros, añadiéndole a los naturales $1,2,3,4,...$ el 0 y otros números con rayas $\overline{1},\overline{2},\overline{3},\overline{4},...$ Los naturales se suman como siempre, los demás se suman así:

$$0+0 = 0$$
$$m+0 = 0+m = m$$
$$\overline{m}+0 = 0+\overline{m} = \overline{m}$$
$$\overline{m}+\overline{n} = m+n-1$$
$$m+\overline{n} = \overline{m}+n = \overline{m+n}$$

   a. Muestra que esta suma definida en el conjunto $\{0,\overline{1},1,\overline{2},2,\overline{3},3,\overline{4},4,...\}$ es conmutativa, asociativa y tiene un neutro aditivo, pero no hay inversos aditivos. ¿se vale la cancelación?
   b. A estos números raros ya los conocen, pero de otra forma. ¿pueden adivinar quienes son?

El orden en **Z**.

Decimos que $m<n$ si existe $r \in \mathbf{N}$ tal que $m+r=n$.

Así que $m>0$ si y solo si $m \in \mathbf{N}$ y $m<0$ si y solo si $-m>0$. Esto define un **orden** en **Z** que extiende el orden definido anteriormente en **N**. El orden en **Z** tiene las siguientes propiedades:

- Si $m<n$ y $n<p$ entonces $m<p$
- Si $m<n$ entonces $m+p<n+p$ para cada p
- Si $m<n$ y $p>0$ entonces $mp<np$ y si $p<0$ entonces $mp>np$

Las dos primeras propiedades se prueban igual que en **N**, para la ultima hay que usar que el producto de dos naturales es un natural, así que si $m>0$ y $n>0$ entonces $m \cdot n>0$.

Ejercicio. Si m,n,p,q son enteros con $m<n$ y $p<q$ ¿será cierto que $mp<nq$?

Otra representación de **Z** a partir de **N**.

Podemos representar a los números enteros usando *parejas* de naturales, haciendo que la pareja (m,n) represente al entero $m-n$. En particular, la pareja (m,m) representa al 0.

Hay muchas parejas que representan al mismo entero: (m,n) y (m',n') representan lo mismo si $m-n=m'-n'$ o sea si $m+n'=m'+n$.

Si ahora definimos una relación de equivalencia entre parejas, diciendo que $(m,n) \sim (m',n')$ si $m+n'=m'+n$ entonces obtenemos una biyección entre los números enteros y las clases de equivalencia de parejas.

¿Como se verán la suma y la multiplicación de enteros vistos como parejas de naturales?

- Como (m,n) representa a $m-n$ y (o,p) representa a $o-p$ entonces $(m,n)+(o,p)$ debe representar a $m-n+o-p$, así que $(m,n)+(o,p)=(m+o,n+p)$.
- Como $(m,n) \cdot (o,p)$ debe representar a $(m-n) \cdot (o-p)=mo+np-mp-no$, entonces $(m,n) \cdot (o,p) = (mo+np,mp+no)$.

Esta representación de los números enteros puede parecer rebuscada, pero así todos los elementos de **Z** tienen la misma forma, no hay que definir la suma y la multiplicación por casos, y se ve que las propiedades conmutativas, asociativas y distributivas en **Z** son consecuencia de esas mismas propiedades en **N**.

Problemas.

5. Demuestra a partir de la definición que se cumple la tercera propiedad del orden en **Z**, es decir, que si a, b y c son enteros, a<b y c>0 entonces ac<bc y si a<b y c<0 entonces ac>bc.

6. Demuestra que en **Z**, a<b no implica que $a^2<b^2$, pero si implica que $a^3<b^3$.

$a<b \Rightarrow a^3<b^3$:

1. Si a y b tienen distinto signo. Entonces $a<0$ y $0<b$ así que $a^3=a\cdot a^2<0\cdot a^2=0=0\cdot b^2<b\cdot b^2=b^3$
2. Los casos $a=0$ o $b=0$ salen cambiando una de las desigualdades anteriores por igualdad.
3. Si a y b tienen el mismo signo. Entonces $ab>0$ así que en la igualdad

$a^3+a^2(b-a)+ab(b-a)+b^2(b-a)= b^3$ las 3 cantidades en rosa son positivas, por lo tanto $a^3< b^3$.

7. Usando la representación de los enteros como parejas de naturales, muestra que:

a. el producto en **Z** es asociativo.
b. existe un neutro multiplicativo.
c. el producto en **Z** se distribuye con la suma.

Divisibilidad

Decimos que un entero **m** **divide** a un entero **n**, y escribimos **m|n**, si existe **c** en **Z** tal que **mc=n**.

Ejemplos.

- 2|6 ya que 2·3=6
- 0|0 ya que 0·1=0
- 0 no divide a ningún b≠0, porque no existe c tal que 0·c=b.

Lema 1. Si **m** y **n** son enteros positivos y **m|n** entonces **m≤n**.

Demostración. Si **m|n** entonces existe un entero **c** tal que **mc=n**. Como **m>0** y **n>0** entonces **c>0**.
Para ver que **m≤n** si tenemos que ver que existe un entero **d≥0** tal que **m+d=n**.
Como **mc=n** entonces **m+m(c-1)=n** y el número **d=m(c-1)** es mayor o igual a **0** (ya que **m>0** y **c>0**, así que **c≥1** por lo tanto **c-1≥0**). Como **m+d=n** con **d≥0**, entonces **m≤n**. □

El algoritmo de la división. Si **m** y **n** son números enteros con **m>0**, entonces existe un único par de enteros **c** y **r** tales que **n=mc+r** con **0≤r<m**.

Demostración. Consideremos todos los múltiplos (positivos y negativos) de m, y elijamos el mayor de ellos, digamos mc, que sea menor o igual a n. Entonces $mc\le n<m(c+1)$, ya que de otro modo $m(c+1)$ seria un múltiplo aun mayor de m que es menor o igual que n. Restando mc a la desigualdad queda $0\le n-mc<m$, y si hacemos $r=n-mc$ entonces $n=mc+r$.

Para ver que solo existe un par de enteros c y r tales que $n=mc+r$ y $0\le r<m$, supongamos que existiera otro par c', r' tales que $n=c'm+r'$ con $0\le r<m$.

Restando las dos expresiones para n obtenemos $mc+r=mc'+r'$ así que $mc-mc'=r'-r$ o sea $m(c-c')=r'-r$.

Esto dice que $r-r'$ es un múltiplo de m. Pero $r<m$ y $r'<m$, así que $0\le r-r'<m$ o $0\le r'-r<m$, así que por el lema 1, $r-r'=0$. Pero entonces $m(c-c')=0$ y como $m>0$, entonces $c-c'=0$ así que $c=c'$. □

Ejemplos. Dividir

17 entre 3	-17 entre 3	3 entre 17	-3 entre 17
$17=5\cdot3+2$	$-17=-6\cdot3+1$	$3=0\cdot17+3$	$-3=-1\cdot17+14$
cociente, residuo	cociente, residuo		

Si **m** y **n** son enteros, las **combinaciones lineales enteras** de **m** y **n** son todos los números de la forma **rm+sn** con **r** y **s** enteros.

Ejemplo. Algunas combinaciones lineales enteras de 3 y 7 son

$10=3+7$ $\quad -4=3-7$ $\quad 3=(1)3+(0)7$ $\quad -2=(4)3+(-2)7$

Lema 2. Si **a|m** y **a|n** entonces **a** divide a todas las combinaciones lineales enteras de **m** y **n**.

Demostración. Si $a|m$ entonces $m=ac$ y si $a|n$ entonces $n=ad$ para algunos c y d en **Z**.

Así que $rm+sn = r(ac)+s(ad) = a(rc+sd)$ y por lo tanto $a|rm+sn$. □

Lema 3. Si **m** y **n** son dos enteros distintos de **0**, entonces existe una combinación lineal entera de **m** y **n** que divide a **m** y también a **n**.

Demostración. Consideremos todas las combinaciones lineales enteras *positivas* de m y n y elijamos la menor de ellas, digamos que es $c=rm+sn$. Afirmamos que c divide a m y a n.

Si c no dividiera a m, entonces por el algoritmo de la división podríamos escribir $m=tc+u$, donde $0<u<c$.

Entonces $m=t(rm+sn)+u$ así que $u=(1-tr)m-tsn$, por lo tanto u es una combinación lineal de m y n que es positiva y es menor que c, y esto es una contradicción El mismo argumento demuestra que c divide a n. □

El **máximo común divisor** (**mcd**) de dos enteros **m** y **n** es el mayor entero que divide a **m** y **n**.

Ejemplo. El mcd de 8 y 12 es 4. El mcd de 9 y 10 es 1. Pero hallar el mcd de números mas grandes no es tan fácil. ¿Cual será el mcd de 901 y 493?

Lema 4. Si **m** y **n** son dos enteros positivos entonces

a. El mcd de **m** y **n** es la menor de las combinaciones lineales enteras positivas de **m** y **n**.
b. El mcd de **m** y **n** es divisible entre todos los divisores comunes de **m** y **n**.
c. Las combinaciones lineales enteras de **m** y **n** son los múltiplos del mcd de **m** y **n**.

Demostración.

a. Sea c la menor de todas las combinaciones lineales enteras positivas de m y n. Veremos que c es su mcd. Por el lema 2, los divisores comunes de m y n dividen a las combinaciones lineales enteras de m y n, así que su mcd divide a c. Pero por el lema 3 la menor combinación lineal entera positiva de m y n, que es c, divide a m y n. Así que c es menor o igual a su mcd. Por lo tanto c es su mcd.

b. Por el lema 2 todos los divisores comunes de m y n, dividen a todas las combinaciones lineales enteras de m y n, y ya probamos en a. que el mcm es una de estas combinaciones.

c. Por el lema 2 todas las combinaciones lineales enteras de **m** y **n** son divisibles entre los divisores de m y n, así que son múltiplos del mcd de m y n. Por a. el mcd es una combinación lineal de m y n, así que todos sus múltiplos son combinaciones lineales de m y n. •

Decimos que dos enteros **m** y **n** son **primos relativos** si el mcm de **m** y **n** es 1.

Ejemplos. 99 y 101 son primos relativos. 99 y 102 no son primos relativos.
¿221 y 299 serán primos relativos o no?

Corolario. Dos enteros **m** y **n** son primos relativos si y solo si existen enteros **a** y **b** tales que **am+bn=1**.

Problemas.

8. ¿Cual es el resultado de la división? da el cociente y el residuo
   a. 29 entre 11 b. -29 entre 11 c. $1-n^2$ entre n d. $(n-1)^2$ entre n

9. Encuentra una combinación lineal entera de 7 y 9 que de 3 y otra que de -4.

10. Encuentra una combinación lineal entera de los dos números que divida a ambos.
    a. 5 y 8 b. 15 y 21 c. 13 y 22

11. Demuestra *directamente* (sin usar los lemas) que todas las combinaciones lineales enteras de dos números son múltiplos de su combinación lineal entera positiva mas pequeña.

12. ¿Como definirías al mcd de 3 enteros? ¿Será cierto que el mcd de 3 enteros es una combinación lineal entera de los tres?

13. Demuestra que cualesquiera dos impares consecutivos son primos relativos.

14. Si en lugar de pensar en números enteros pensamos en fracciones m/m y en sus múltiplos enteros. ¿Como son todas las combinaciones lineales enteras de 1/2 y 2/3? ¿Es verdad que todas estas son múltiplos de una sola fracción?

El algoritmo de Euclides es un método muy eficiente para calcular el máximo común divisor de dos enteros positivos sin tener que hallar los divisores de cada uno. Este algoritmo se ha usado durante mas de 2400 años.

Algoritmo de Euclides. Si **m** y **n** son dos enteros positivos con **m<n** entonces el mdc de **m** y **n** es el mismo que el mcd de **m** y **n-m** (ejercicio) y esto reduce el mayor de los 2 números.
Si ahora tomamos a **m** y **n-m** y al mayor le restamos el menor volvemos a reducir el mas grande sin cambiar el mcd.
Podemos repetir el proceso con los números resultantes hasta que los dos números sean iguales, y por lo tanto sean iguales a su mcd, que es el mcd de **m** y **n**.

Este proceso de resta consecutiva se puede abreviar usando el algoritmo de la división: si dividimos **n** entre **m** y queda resto **r**, entonces **r** y **m** tienen el mismo mcd que **m** y **n** (ejercicio).
Si ahora dividimos **m** entre **r** y queda resto **s**, **s** y **r** tienen el mismo mcd que **r** y **m**.
Podemos seguir dividiendo hasta que no haya residuo, y el mcd de **m** y **n** es el ultimo residuo distinto de 0.
Si invertimos este procedimiento, podemos obtener el mcd de **m** y **n** como combinación lineal entera de **m** y **n**.

Ejemplo. Hallar el mcd de 168 y 45

$$
\begin{aligned}
168 &= 3\cdot 45+33\\
45 &= 1\cdot 33+12\\
33 &= 2\cdot 12+9\\
12 &= 1\cdot 9+3\\
9 &= 3\cdot 3
\end{aligned}
$$

así que el mcd de 168 y 45 es 3.

Para expresar al mcm como combinación lineal vamos en reversa desde la penúltima igualdad, reemplazando en cada paso los residuos por las combinaciones lineales del dividendo y el divisor que los producen:

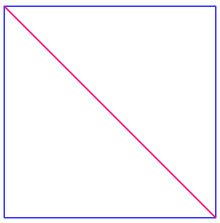
$$
\begin{aligned}
3 &= 12-1\cdot 9\\
&= 12-1\cdot(33-2\cdot 12)\\
&=-1\cdot 33+3\cdot 12\\
&=-1\cdot 33+3\cdot(45-1\cdot 33)\\
&= 3\cdot 45-4\cdot 33\\
&= 3\cdot 45-4(168-3\cdot 45)\\
&=-4\cdot 168+15\cdot 45
\end{aligned}
$$

esta es la combinación lineal entera de 168 y 45 que da 3.

Podemos tratar de usar el algoritmo de Euclides para hallar geométricamente el mcd de dos magnitudes arbitrarias a y b, es decir, la mayor magnitud que multiplicada por algunos enteros de las magnitudes a y b.

El problema es como saber si el proceso se detendrá después de una cantidad finita de repeticiones o si podría continuar indefinidamente, produciendo magnitudes cada vez mas pequeñas.

Esto último sucedería si no existe ninguna magnitud c que divida exactamente a a y b.
Se dice que 2 magnitudes son *conmensurables* si tienen un divisor común, si no lo tienen se llaman *inconmensurables*.



El lado y la diagonal de un cuadrado son inconmensurables, ya que √2 es irracional.

Problemas.

15. Usa el algoritmo de Euclides para hallar el mdc de los 2 números y halla una combinación lineal de ellos que de el mcd.

    a. 91 Y 117 b. 56 y 189 c. 220 y 273 d. 10,001 y 100,001

16. Usa el algoritmo de Euclides y una calculadora para hallar el mcd de los 2 números.

    a. 1386 y 3213 b. 123456789 y 987654321

17. ¿Que relación hay entre el mcd de **m** y **n** y el mcd de **m+n** y **m-n**? Haz varios ejemplos para ver que ocurre y haz una conjetura de lo que debe pasar en todos los casos.

18. Escribe un programa (en Python por ejemplo) que calcule el mcd de 2 números.

19. El *mínimo común múltiplo* de **m** y **n** es el menor entero positivo que es divisible entre **m** y **n.**
    a. Muestra que el mcm de **m** y **n** es una combinación lineal de entera de **m** y **n**.
    b. Demuestra que el mcm divide a todos números enteros que son divisibles entre **m** y **n**.

Números Primos.

Un número natural p mayor que 1 es primo si no es producto de dos números naturales menores que p, es decir, si los únicos naturales que dividen a p son 1 y p. Los números naturales mayores que **1** que no son primos se llaman *compuestos*.

Ejercicio. ¿Cuales de los siguientes números son primos y cuales son compuestos?

83 91 111 159 197

La Criba de Eratostenes es un algoritmo para encontrar todos los primos.
En la lista de los enteros positivos tomar el primer número mayor a 1 (el 2) y marcar sus múltiplos, luego fijarse el siguiente número no marcado (el 3) y marcar sus múltiplos, y en cada paso subsecuente tomar el siguiente número no marcado y pintar sus múltiplos. Los primos son todos los números no marcados.

En la siguiente lista los múltiplos de 2 están marcados de naranja, los múltiplos de 3 (que no son múltiplos de 2) están marcados de verde, los múltiplos de 5 (que no son múltiplos de 2 o 3) están marcados de azul, los múltiplos de 7 (que no son múltiplos de 2, 3 o 5) están marcados de morado, etc. Los primos son los números que quedan sin marcar (en negro).

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59
60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87
88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112

Lema (Euclides). Si un primo **p** divide al producto de dos enteros **m** y **n** entonces **p** divide a **m** o **p** divide a **n.**

Demostración. La demostración original de Euclides era complicada, la demostración moderna es simple: Supongamos que **p** divide a **mn.** Como **p** es primo, si **p** no divide **m** entonces el máximo común divisor de **p** y **m** es 1. Así que por el lema 3 existen dos enteros **a** y **b** tales que **ap+bm=1** .Multiplicando la igualdad por **n** obtenemos **apn+bmn=n**. Como **apn** y **mnb** son divisibles entre **p** entonces su suma, que es **n**, es divisible entre **p**. □

Corolario. Si un primo **p** divide a un producto de enteros $n_1n_2...n_k$ entonces **p** divide a algún n_i.

Demostración. Por el lema de Euclides si **p** divide a $n_1n_2...n_k$ entonces **p** divide n_1 o **p** divide a $n_2...n_k$. En el primer caso ya acabamos. Si **p** divide a $n_2...n_k$ entonces **p** divide a n_2 o **p** divide a $n_3...n_k$, y podemos repetir el argumento hasta llegar a que **p** divide a algún n_i o concluir que **p** divide a n_k. □

Teorema fundamental de la aritmética. Si **n** un número natural mayor que 1 entonces **n** se puede factorizar como producto de números primos, y la factorización es única salvo por el orden de los factores.

Demostración. Veremos primero que la factorización siempre existe, usando inducción sobre **n**. 2 es primo porque los únicos números que lo dividen son 1 y 2. Supongamos ahora que los números menores que **n** se pueden factorizar como producto de primos y veamos que pasa con **n**.

Si **n** es un primo ya acabamos, si no, entonces **n** es el producto de dos enteros n_1 y n_2 menores que **n**. Por hipótesis de inducción cada uno es producto de primos, $n_1=p_1p_2 \dots p_r$ y $n_2= q_1q_2 \dots q_s$, y por lo tanto $n = n_1n_2 = p_1p_2...p_rq_1q_2...q_s$ así que **n** también es un producto de primos.

Veremos ahora que la factorización es única (salvo por el orden de los factores) usando inducción sobre **n**. Para el numero **2** es inmediato porque no tiene otros divisores que 1 y 2. Supongamos ahora que todos los números menores que **n** tienen una factorización única my veamos que ocurre para **n**.

Sean $n=p_1p_2 \dots p_r$ y $n=q_1q_2 \dots q_s$ dos factorizaciones primas de **n**. Como p_1 es primo y divide a **n** entonces por el lema de Euclides p_1 divide a algún q_j. Como q_j es primo entonces $p_1=q_j$. Ahora podemos dividir a **n** entre $p_1=q_j$: El resultado es un número $m<n$ que tiene dos factorizaciones primas: $m=p_2 \dots p_r$ y $m=q_1q_2...q_{j-1}q_{j+1}...q_s$. Por hipótesis de inducción estas factorizaciones de **m** son iguales, salvo por el orden de los p_i's y q_j's. Así que las dos factorizaciones de **n** que se obtienen añadiendo el factor $p_1=q_j$ a las factorizaciones de **m**) son iguales salvo por el orden. □

Ejercicio. Encontrar la factorización prima de los siguientes números:

93 187 201 299 323 666 1001

Corolario. El máximo común divisor de **m** y **n** es el producto de todos los primos que aparecen tanto en las factorización de **m** como la de **n**, con las repeticiones que aparezcan en las dos.

Ejemplo: ¿Cual es el mcd de 252 y 120?

$252=2^2\cdot 3^2\cdot 7$ y $120=2^3\cdot 3\cdot 5$ así que el mcd de 252 y 120 es $2^2\cdot 3=12$

Teorema (Euclides). Existen una infinidad de números primos.

Demostración. Supongamos que existieran solo un número finito de primos, digamos $\mathbf{p_1, p_2,\ldots, p_n}$. Considérese el número $\mathbf{n=p_1p_2\ldots p_n+1}$. Entonces **n** no puede ser dividido por ningún $\mathbf{p_i}$, ya que si lo fuera $\mathbf{p_1}$ dividiría a $\mathbf{n-p_1p_2\ldots p_n=1}$. Así que **n** debe ser primo o debe ser un producto de primos distintos de $\mathbf{p_1, p_2,\ldots, p_n}$, contradiciendo que en esa lista estaban todos los primos. □

¿Existirán fórmulas para obtener puros números primos?
Euler encontró un polinomio que da muchos primos: $p(n)=n^2+n+41$
p(1)=43 p(2)=47 p(3)=53 p(4)=61 p(5)=71 p(6)=83
¿pueden hallar un valor de n para el que p(n) no sea primo?

Problemas.

18. Ejercicio. ¿Cuales de estos números son primos y cuales son compuestos?

a. 101 b. 1001 c. 10001 d. 100001 e. 123456

19. Encuentra la factorización prima de los siguientes números

a. 111 b. 143 c. 197 d. 231 e. 299 f. 639

20. Muestra que $\mathbf{p(n)=n^2+n+11}$ es primo para todos los naturales menores que 10.
¿Para cuales naturales menores que 12 $\mathbf{q(n)=n^2+n+13}$ es primo?

21. Demostrar que si **a** y **b** son primos relativos y **a|bc** entonces **a|c** (**a** no tiene que ser primo).
Hint: entender la demostración el lema de Euclides.

22. Demostrar que si **a** y **b** son dos números naturales, **m** es su máximo común divisor y **n** es su mínimo común múltiplo, entonces **ab = mn**. Hint: factorizar a **a** y **b** como productos de primos y ver cuales factores aparecen en **m** y en **n**.

23. *Demuestra que si $\mathbf{2^p-1}$ es primo, entonces **p** debe ser primo.

24. Usando la descomposición prima, demuestra que no existen números naturales **m** y **n** tales que $\mathbf{2m^k=n^k}$ para ningún natural k>1.

Ecuaciones diofantinas.

Una **ecuación diofantina** es una ecuación a la que se buscan solamente soluciones enteras. Las mas simples son las ecuaciones lineales **ax+by=c** donde **a**, **b**, **c** son enteros y buscamos soluciones con **x** y **y** *enteros*.

Ejemplo. ¿La ecuación diofantina $6x+9y=33$ tiene soluciones enteras?

En este ejemplo podemos hallar al tanteo una solución: $x=4$, $y=1$.

¿La ecuación $6x+9y=35$ tiene soluciones enteras?

No, Si existiera una solución 35 seria una combinación lineal entera de 6 y 8, pero el mcd de 6 y 9 es 3, así que todas sus combinaciones enteras $6x+9y$ son divisibles entre 3, pero 35 no lo es.

Lema. La ecuación diofantina **ax+by=c** tiene soluciones si y solo si el mcd de **a** y **b** divide a **c**.

Demostración. $\Rightarrow$ Si existe una solución entera de la ecuación $ax+by=c$ entonces c es una combinación lineal entera de a y b, por lo tanto c es divisible entre el mcd de a y b.
$\Leftarrow$ Δi el máximo común divisor de a y b es d, entonces d es una combinación lineal entera de a y b y por lo tanto cualquier múltiplo de d es una combinación lineal entera de a y b. •

Ejemplo. ¿Existen soluciones enteras de la ecuación $5x+7y=4$?

Como el mcd de 5 y 7 es 1, que divide a 4, la ecuación si tiene soluciones.
1 es combinación lineal entera de 5 y 7: $5(3)+7(-2)=1$ y como 4 es múltiplo de 1, 4 también es combinación lineal de 5 y 7: $5(12)+7(-8)=4$.
Así que $x=12$, $y=-8$ es una solución entera de la ecuación $5x+7y=4$.

Ahora nos preguntamos cuantas soluciones enteras puede tener una ecuación **ax+by=c** y como podemos hallarlas todas. Primero pensemos en las ecuaciones homogéneas **ax+by=0.**

Lema. Las soluciones de la ecuación diofantina **ax+by=0** son $\mathbf{x = {}^{b}/_{d}m}$, $\mathbf{y= -{}^{a}/_{d}m}$ donde **d** es el mcd de **a** y **b** , y donde **m** es cualquier numero entero.

Demostración. La ecuación puede escribirse como $ax=-by$ lo que dice que a divide a by y b divide a ax.
Caso 1. Si el mcd de a y b es 1, entonces a divide a y y b divide a x. Así que $y=am$ y $x=bn$ y como $abn=-bam$ asi que $n=-m$. Y $x=bm$, $y=-am$ nos da una solución para cada entero m.

Caso 2. Si el mcd de a y b es d, podemos dividir a y b entre d. La ecuación $ax+by=0$ tiene las mismas soluciones que $ {}^{a}/_{d}\, x + {}^{b}/_{d}\, y = 0$, donde $ {}^{a}/_{d}$ y $ {}^{b}/_{d}$ son enteros y su máximo común divisor es 1.
Por el caso 1 las soluciones de esta ecuación son de la forma $x = {}^{b}/_{d}\, m$, $y = -{}^{a}/_{d}\, m$. •

Ejemplo. ¿Cuales son todas las soluciones de la ecuación diofantina $6x+8y=0$?

El mcd de 6 y 8 es 2, así que podemos dividir la ecuación entre 2 y obtener la ecuación equivalente $3x+4y=0$ donde los coeficientes 3 y 4 son primos relativos, por lo que las soluciones son $x=4m$, $y=-3m$ para $m \in \mathbf{N}$.

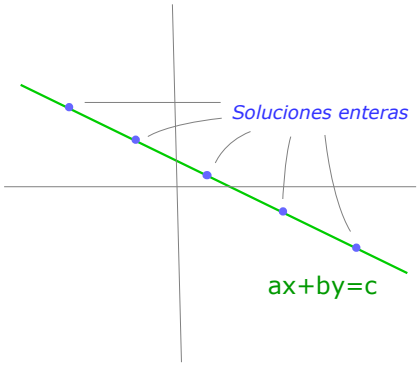
Lema. Las soluciones de la ecuación diofantina **ax+by=c** son las sumas de soluciones de la ecuación homogénea **ax+by=0** con alguna solución particular de la ecuación original, suponiendo que esta solución existe.

Demostración. Si (m,n) y (m',n') son dos soluciones de ax+by=c, entonces am+bn=c y am'+bn'=c así que a(m-m')+b(n-n')=0 lo que dice que (m-m',n-n') es una solución de la ecuación homogénea ax+by=0.
Así que (m',n') es la suma de una solución particular (m,n) con una solución de la ecuación homogénea.
Recíprocamente, si (m,n) es una solución de la ecuación original, ax+by=c, y (r,s) es una solución de la ecuación homogénea, ax+by=0 entonces sumandolas queda a(m+r)+b(n+s)=c lo que dice que (m+r,n+s) es otra solución de la ecuación original. •

Ejemplo. ¿Cuales son todas las soluciones enteras de la ecuación 5x+7y=4?

Ya vimos que una solución de la ecuación es x=12 , y=-8.
Las otras soluciones se obtienen sumándole a esta solución las soluciones de la ecuación homogénea 5x+7y=0. Sabemos que las soluciones de 5x+7y=0 son x=7m, y=-5m para m ∈ **N**, así que las soluciones de 5x+7y=4 son de la forma x=12+7m, y=-8-5m para m ∈ **N**.
Podemos comprobar que 5(12+7m)+7(-8-5m) = 60+35m-56-35m = 4.

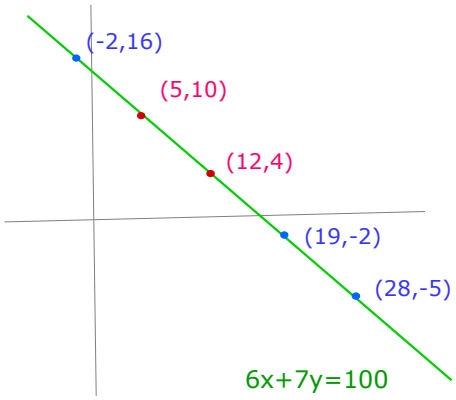
Por los lemas anteriores cada ecuación lineal diofantina **ax+by=c** tiene una cantidad infinita de soluciones enteras o no tiene ninguna solución entera
Las soluciones enteras corresponden a los puntos con coordenadas enteras de la recta definida por la ecuación.



A veces nos interesan solamente las soluciones positivas (o no negativas) de una ecuación diofantina. La existencia de soluciones enteras *no implica* la existencia de soluciones no negativas, pero teniendo todas las soluciones enteras es fácil localizar las que nos interesan.

Ejemplo. ¿Es posible dividir a un grupo de 100 estudiantes en equipos de 6 o 7 personas?

Queremos soluciones de la ecuación 6x+7y=100 con x, y enteros no negativos.
Las soluciones enteras existen porque el mcd de 6 y 7 es 1, que divide a 64: como 6(-1)+7(1)=1 entonces 6(-100)+7(100)=130.
Las otras soluciones de la ecuación se obtienen sumandole las soluciones de la ecuación homogénea 5x'+7y'=0 que son x'=7n, y'=-6n.
Así que las soluciones enteras de 6x+7y=100 son x=-100+7n, y=100-6n, n.
Para que x, y sean no negativos -100+7n>0 y 100-6n>0, o sea n>130/7=14.28... y n<130/6=16.66...
Asi que n=15 o n=16, lo que da x=5, y=10 o x=12, y=4.
Y esto dice que hay 2 maneras de partir el grupo
(5 equipos de 6 y 10 equipos de 7 o 12 equipos de 6 y 4 de 7)



Problemas.

25. En un frasco hay hormigas y arañas ¿Cuantas hormigas y cuantas arañas pueden haber si en total hay 82 patas? (den todas las soluciones)

26. ¿Que cantidades se pueden pagar con billetes de 20 y 50 pesos, si no dan cambio?

27. ¿Que cantidades se pueden pesar en una balanza, si se dispone de muchas pesas de 1/2 kilo y de 1/3 de kilo, y las pesas se pueden poner en los dos lados de la balanza?
¿Y si las pesas solo se pueden poner de un lado?

28. Encuentra *todas* las soluciones enteras de las siguientes ecuaciones:

a. $3x-8y=1$ b. $5x+7y=38$ c. $4x+6y=18$ d. $9x+12y=27$

29. Encuentra las soluciones enteras positivas de las ecuaciones anteriores.

30. Demuestra que si a y b son primos relativos, entonces cada número natural n es la diferencia entre un múltiplo de a y uno de b, es decir, $ax-by=n$ tiene soluciones enteras positivas.

31.* ¿Es verdad que si a y b son primos relativos entonces existe un número a partir del cual todos los números naturales son la suma de un múltiplo positivo de m y uno de n?