Divisibilidad (en $\mathbb{N}^* = \mathbb{N} \cup \{0\}$)

* Dados dos números naturales a y c, se dice que c es un divisor de a si existe $q \in \mathbb{N}^*$ tal que $a = q \times c$

  (es decir, si en la división $a \div c$ el resto es 0).

  $c \mid a$ significa que c es divisor de a.

  Ejemplos:

  - $2 \mid 14$ porque $14 = 7 \times 2$.
  - $7 \mid 91$ porque $91 = 13 \times 7$.

* Si c no es divisor de a, escribiremos $c \nmid a$.

  Ejemplos:

  - $2 \nmid 15$ porque $15 = 7 \times 2 + 1$.
  - $7 \nmid 95$ porque $95 = 13 \times 7 + 4$.

* El 0 y los divisores:

  ¿ $2 \mid 0$? ¿ $0 \mid 3$?

* Múltiplos y divisores

  Si $c \mid a$, también decimos que a es múltiplo de c.

  Ejemplos:

  - $2 \mid 14 \rightarrow 14$ es múltiplo de 2.
  - $7 \mid 91 \rightarrow 91$ es múltiplo de 7.

* Denotamos por $\dot{c}$ al conjunto de los múltiplos de c.

  Ejemplo: $\dot{3} = \{0, 3, 6, 9, 12, \ldots\}$.

Divisibilidad

* Ejercicio: escribe todos los divisores de 20.

* Dado cualquier número natural n, los números 1 y n son siempre divisores de n. Al resto de divisores, se les llama divisores propios.

* Def: Decimos que un número natural $p > 1$ es un número primo si no tiene divisores propios (es decir, si sus únicos divisores son 1 y p).

* Hay una buena razón para no considerar $p = 1$ como número primo (la veremos pronto).

  Una alternativa para no tener que hacerlo de forma explícita:

  Def: Un número es primo si tiene exactamente dos divisores.

* Un número que no es primo diremos que es compuesto.

Números primos: preguntas básicas

* ¿Es n un número primo?

  a) ¿Es 97 un número primo?

  b) ¿Es 883 un número primo?

  ¿Cuándo podemos dejar de buscar divisores?

* Encuentra todos los números primos menores que n:
  la criba de Eratóstenes.
  http://www.visnos.com/demos/sieve-of-eratosthenes

* Ejercicio: Adapta la criba de Eratóstenes para encontrar los números primos mayores que 170 y menores que 200.

Descomposición en factores primos (Factorización)

* Es fácil convencerse de que cualquier número se puede poner como producto de números primos.

  Ejemplo: $364 = 2 \times 182 = \cdots = 2^2 \times 7 \times 13$

364	2
182	2
91	7
13	13
1	

Algoritmo tradicional (en España)

* Los números primos son los "ladrillos" que forman el resto de los números.

  Veremos que conocer la factorización de un número nos da mucha información.

Descomposición en factores primos (Factorización)

* Teorema fundamental de la aritmética:
  Todo número entero se puede escribir,
  de manera única, como producto de números primos.

* Demostrar que se pueden descomponer es muy sencillo:
  Si n es primo, hemos terminado.
  Si no, tiene algún divisor a, y tenemos que $n = a \cdot b$. Ahora podemos repetir el razonamiento con a y b.

  Que hay solo una descomposición (salvo el orden, claro) no es tan inmediato, y no lo vamos a demostrar.

Factores primos y divisores

* Ejercicio: Escribe todos los divisores de 60 y compara la factorización de 60 con la factorización de sus divisores.

* En general:

$$245\,784 = 2 \times 2 \times 2 \times 3 \times 7 \times 7 \times 11 \times 19$$

$2 \times 7 \times 7 \times 19 = 1862$ es un divisor de $245\,784$

* La factorización de un número nos da toda la información sobre sus divisores.

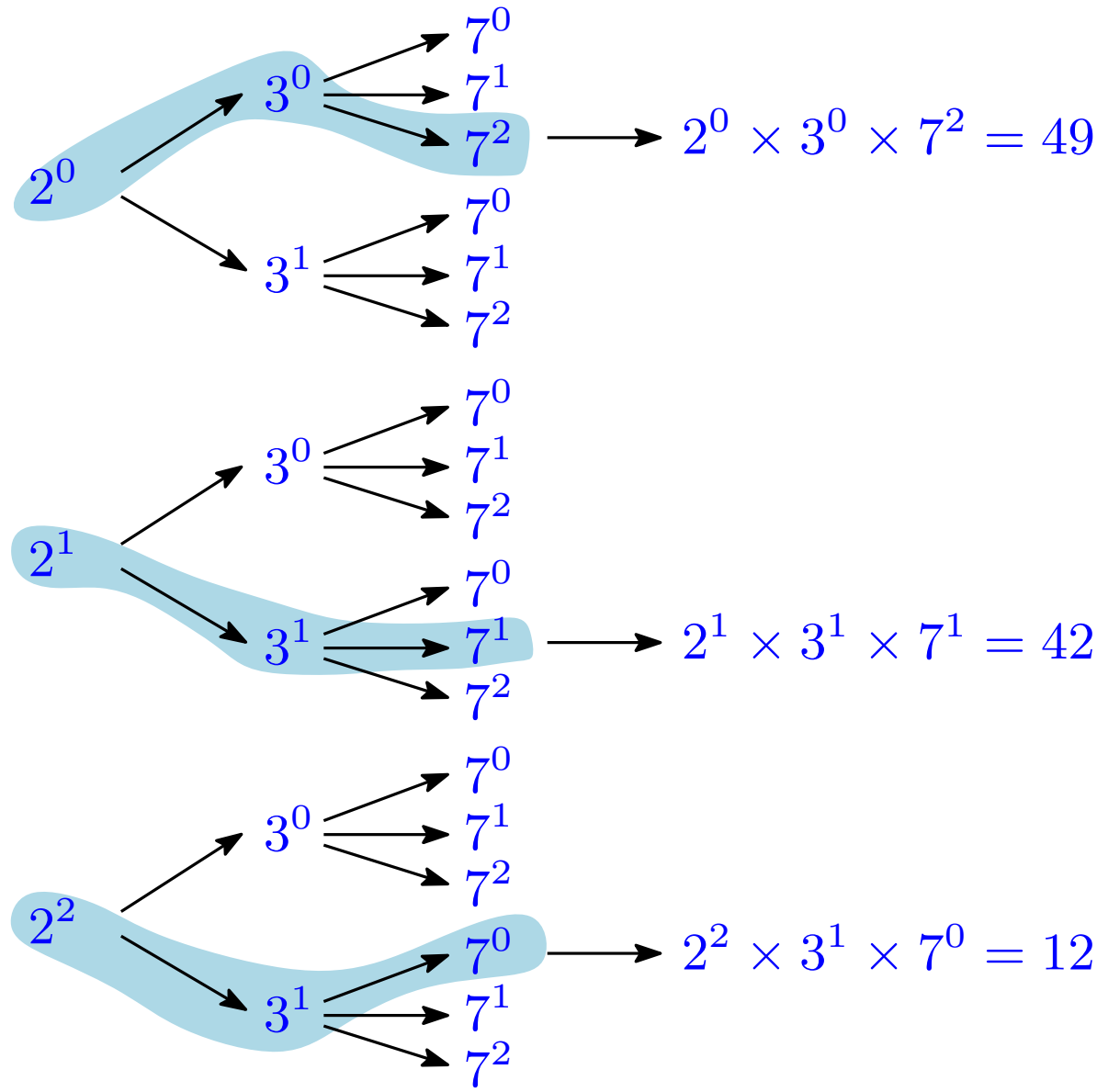
  Una buena forma de verlo es organizar los divisores en un árbol.

Factores primos y divisores

* Ejemplo:

  $588 = 2^2 \times 3 \times 7^2$.

  Árbol de sus divisores.



Factores primos y divisores

* Este árbol nos permite contestar a preguntas como las siguientes: (fíjate que para contestar estas preguntas no hace falta construir el árbol completo)

  1. ¿Cuántos divisores tiene el número?
  2. ¿Cuántos divisores son pares/impares/múltiplos de ...?
  3. Escribe los divisores que son múltiplos de 28.

* La mejor forma de comprobar que lo has entendido es hacer este ejercicio:

  Sabiendo que $5720 = 2^3 \times 5 \times 11 \times 13$,

  1. ¿cuántos divisores tiene el número 5720?
  2. escribe los divisores impares de 5720.
  3. ¿cuántos divisores de 5720 son múltiplos de 22?

El número de divisores

* Observa que hemos obtenido esta fórmula para el número de divisores:

  Si $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k}$ entonces n tiene

  $(a_1 + 1) \times (a_2 + 1) \times \cdots \times (a_k + 1)$ divisores.

  (Si has entendido la transparencia anterior, no hace ninguna falta que memorices esta fórmula).

El razonamiento "al revés"

* Una buena forma de profundizar en la comprensión de un tema es trabajar el razonamiento "al revés".

  Hemos visto cómo, a partir de la factorización, se pueden conocer cosas sobre los divisores.
  En los siguientes ejercicios hay que razonar "al revés":
  a partir de propiedades de los divisores, obtener la factorización.

1. Encuentra 4 números de 3 cifras que tengan 20 divisores.
2. Busca un número que tenga 30 divisores, y tal que 20 de ellos sean números pares.
3. Encuentra el número más pequeño que tiene 8 divisores.

Otras aplicaciones de la factorización

* Encuentra el menor número por el que hay que multiplicar a 140 para que el resultado sea un cuadrado perfecto.

* Encuentra el menor número por el que hay que multiplicar a 360 para que el resultado sea un cubo perfecto.

* Sea $n = 181405$. Sabiendo que $181405 = 71 \cdot 73 \cdot 35$, encuentra la forma de escribir $n = a \cdot b$ $(a, b \in \mathbb{N},\ a > b)$ de manera que $a - b$ sea mínimo.

De vuelta a una pregunta básica

* Teorema (Euclides, $\sim$ 300 aC):

  Existen infinitos números primos.

* Demostración:

  Supongamos que hubiera un número finito. Entonces, podríamos hacer una lista de todos ellos:

  $L = \{p_1, p_2, \ldots, p_n\}$ es la lista de todos los números primos.

  Consideremos el entero $q = p_1 \times p_2 \times \cdots \times p_n + 1$.

  1. q no es un número primo (no está en la lista).
  2. q no se puede poner como producto de factores primos (no tiene divisores en la lista). ¡Imposible!

Comentarios sobre números primos

* Dos impares consecutivos que son ambos números primos se llaman primos gemelos.

  Ejemplos: 3 y 5 son primos gemelos, 11 y 13 también.

* No se sabe si hay una cantidad finita de primos gemelos.

  Los mayores conocidos son $p = 65516468355 \cdot 2^{333333} + 1$ y $p + 2$.

  (Sept. 2013)

  ↓

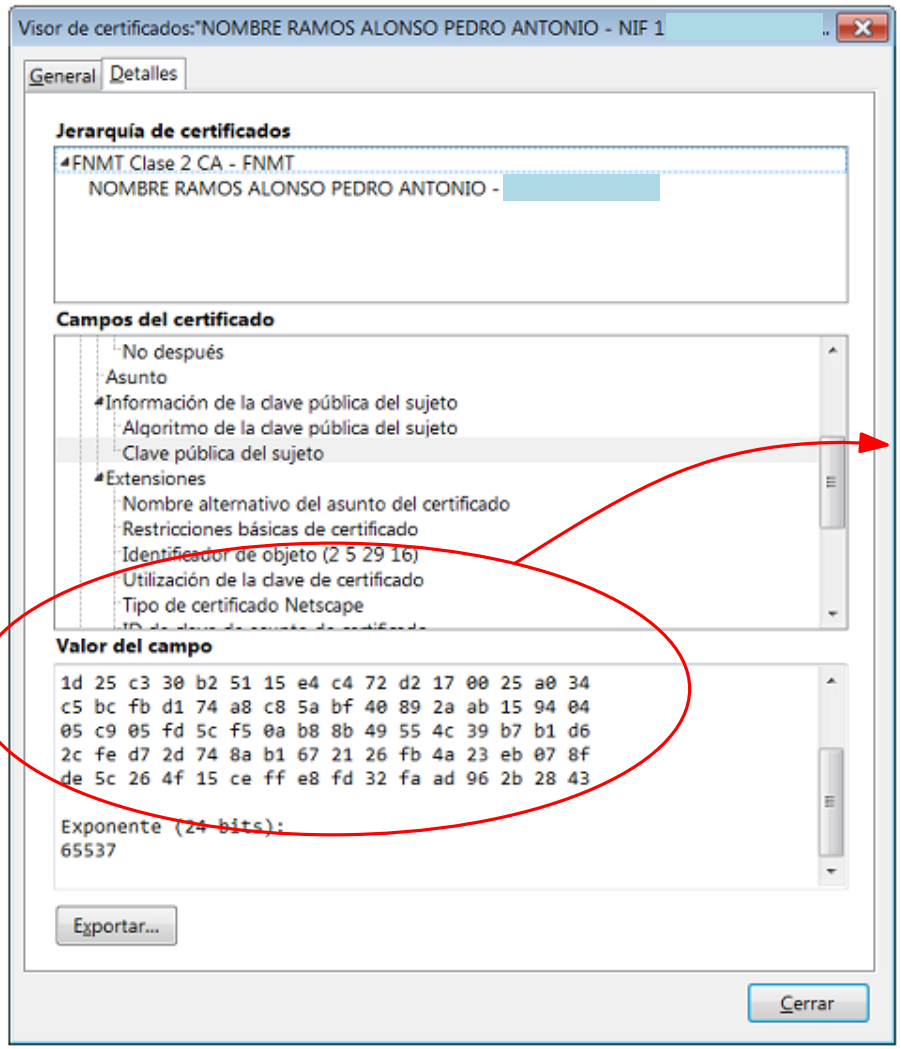
  100355 dígitos

* El mayor número primo conocido (sept. 2013) era

$$p = 2^{43112609} - 1$$

(12978189 dígitos).

Y todo esto, ¿sirve para algo (práctico)?



Buena parte de la seguridad en informática (Internet) depende de que no se sabe descomponer en factores primos números grandes.

RSA: Criptografía de clave pública.
La clave pública de la figura es un número (de aproximadamente 600 dígitos en base 10, pero está expresado en hexadecimal - base 16).

Para leer algo más:
http://es.wikipedia.org/wiki/RSA

Dos propiedades de la divisibilidad

* Si m y n son números pares, entonces $17 \times n + 23 \times m$ también es un número par.

  Esta propiedad se generaliza de la siguiente forma.

* Si a es múltiplo de c, todos los múltiplos de a son también múltiplos de c.

  Equiv: Si $c \mid a$ entonces $c \mid (k \times a)$ (para cualquier k).

* Si a y b son múltiplos de c, entonces $a + b$ también es múltiplo de c.
  Equiv: Si $c \mid a$ y $c \mid b$, entonces $c \mid (a + b)$.

* Combinando estas dos propiedades::
  Si a y b son múltiplos de c, $k \times a + j \times b$ es siempre múltiplo de c.
  Equiv: Si $c \mid a$ y $c \mid b$, entonces $c \mid (k \times a + j \times b)$.

Máximo común divisor

* El máximo común divisor de dos números a y b, $\mathrm{mcd}(a, b)$, es el mayor número natural que es divisor de a y de b.

* ¿Por qué pueden aparecer aquí dificultades de aprendizaje?

  Quizá porque no se pone el suficiente cuidado en diferenciar el concepto en sí mismo del algoritmo para su cálculo.

* Ejercicios:

  a) $\mathrm{mcd}(40, 15)$

  b) $\mathrm{mcd}(38478, 1)$

  c) $\mathrm{mcd}(384787, 0)$

Cálculo de $\mathrm{mcd}(a, b)$

* A partir de la descomposición en factores primos.

  Sabiendo que

$$17640 = 2^3 \times 3^2 \times 5 \times 7^2$$

$$12474 = 2 \times 3^4 \times 7 \times 11$$

  calcula $\mathrm{mcd}(17640, 12474)$.

  (Vamos a pensar, no a tratar de recordar la "receta")

* El máximo común divisor de a y b es el producto de los factores comunes de las descomposiciones en factores primos correspondientes. (Con el menor exponente).

Cálculo de $\mathrm{mcd}(a, b)$

* Obsérvese que de la descomposición en factores primos también se pueden obtener todos los divisores comunes de dos números a y b.

  Encuentra todos los divisores comunes de 17640 y 12474.

* Con la misma idea, se obtiene la siguiente propiedad:

  Los divisores comunes de dos números a y b son los divisores de su máximo común divisor.

* Tenemos una habitación rectangular, de $6{,}30$ m de largo y $4{,}50$ m de ancho. Queremos poner un suelo de baldosas cuadradas, sin tener que partir ninguna baldosa. Si queremos que las baldosas sean del mayor tamaño posible,

  1. ¿de qué tamaño serán las baldosas?
  2. ¿cuántas baldosas necesitaremos?

Máximo común divisor de varios números

* La definición es exactamente igual:

  $\mathrm{mcd}(a_1, a_2, \ldots, a_k)$ es el mayor de sus divisores comunes.

* El algoritmo a partir de la factorización es exactamente el mismo:
  Sabiendo que

$$17640 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$

$$12474 = 2 \cdot 3^4 \cdot 7 \cdot 11$$

$$3591 = 3^3 \cdot 7 \cdot 19$$

$$4998 = 2 \cdot 3 \cdot 7^2 \cdot 17$$

  calcula $\mathrm{mcd}(17640, 12474, 3591, 4998)$.

* Observación: para más de dos números, también es cierto que los divisores comunes de un conjunto de números son los divisores de su máximo común divisor.

Cálculo "mental" del mcd

* ¿Por qué es útil calcular "a ojo" ejemplos como...

  a) $\mathrm{mcd}(9, 24)$
  b) $\mathrm{mcd}(17, 284)$
  c) $\mathrm{mcd}(8, 68)$

* La siguiente propiedad puede ser útil:

  Si k es un divisor de a y de b, entonces

$$\mathrm{mcd}(a, b) = k \cdot \mathrm{mcd}(a/k, b/k).$$

* Ej: calcula $\mathrm{mcd}(84, 24)$.

Mínimo común múltiplo

* El mínimo común múltiplo de dos enteros a y b, que denotaremos $\mathrm{mcm}(a, b)$, es el número natural más pequeño (mayor que cero) que es múltiplo tanto de a como de b.

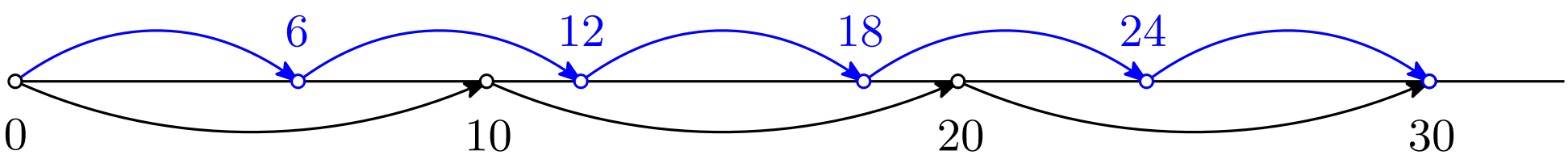
* Las dificultades de aprendizaje son del mismo tipo que las que aparecen con el máximo común divisor.

* Ejercicios:

  a) $\mathrm{mcm}(6, 10)$

  b) $\mathrm{mcm}(29834, 1)$

* La recta numérica es una buena ayuda para la comprensión.



¿Cómo calcular el mínimo común múltiplo?

* En Primaria, a partir de la definición (cálculo mental).

* La divisibilidad en el currículo de la LOMCE (Madrid, 6º)

Divisibilidad. Divisores de un número menor que 100. Máximo común divisor y mínimo común múltiplo.

5. Determina si un número natural cualquiera es múltiplo o divisor de otro.
6. Halla todos los divisores de cualquier número menor que 100.
7. Calcula el m.c.m. y el m.c.d. de dos números naturales.
8. Conoce las reglas de divisibilidad por 2, 3, 5, y 10.
9. Resuelve problemas de recuentos en disposiciones rectangulares y en situaciones en que se aplica la ley del producto.

* La descomposición en factores primos no aparece.

Algoritmo para calcular el mínimo común múltiplo

* Queremos calcular el mínimo común múltiplo de $a = 3591$ y $b = 14994$ sabiendo que

$$3591 = 3^3 \times 7 \times 19$$

$$14994 = 2 \times 3^2 \times 7^2 \times 17$$

(Vamos a pensar, no a tratar de recordar la "receta")

* Idea:

$$3591 \times 14994 = (3^3 \times 7 \times 19) \times (2 \times 3^2 \times 7^2 \times 17)$$

es un múltiplo común. ¿Podemos encontrar alguno más pequeño?

* Propiedad:,

$$\operatorname{mcm}(a, b) = \frac{a \times b}{\operatorname{mcd}(a, b)}$$

Algoritmo para calcular el mínimo común múltiplo

* También hemos obtenido el algoritmo "clásico":

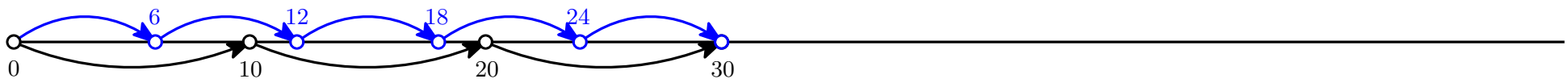
  El mínimo común múltiplo de a y b es el producto de los factores comunes y no comunes, tomando los factores comunes elevados al exponente mayor.

* Este algoritmo sigue siendo válido para calcular el mínimo común múltiplo de más de dos enteros.

  Ojo: no es cierto que $\mathrm{mcd}(a,b,c) \times \mathrm{mcm}(a,b,c)$ sea igual al producto $a \times b \times c$.

Una propiedad del mínimo común múltiplo

* Los múltiplos comunes de dos (o más números) son los múltiplos de su mínimo común múltiplo.



¿Múltiplos comunes de 6 y 10?

* Dos faros emiten una señal especial cada 16 y 12 minutos, respectivamente. Sabiendo que emiten la señal a la vez a las 0 horas y que empezamos a contemplarlos a las 5 de la tarde:
  1. ¿cuántas veces han emitido la señal a la vez antes de que llegáramos?
  2. ¿a qué hora los veremos coincidir por primera vez?

Reglas de divisibilidad

* Aritmética con restos. Un primer ejemplo: par/impar.

* Sea $r(a, n)$ el resto que se obtiene al dividir a entre n.

  Pregunta: si conocemos $r(a, n)$ y $r(b, n)$, ¿podemos determinar $r(a + b, n)$?

* Si $r(a, 3) = 2$ y que $r(b, 3) = 2$, ¿cuánto vale $r(a + b, 3)$?

* Con este tipo de razonamientos, vamos a encontrar las reglas de divisibilidad (de hecho, reglas para calcular restos), para el 3, 4, 5, 6, 8 y 9.

* Ojo: no se podrá usar ninguna regla de divisibilidad adicional, salvo que se justifique adecuadamente.