Divisibility (in $\mathbb{N}^* = \mathbb{N} \cup \{0\}$)

* Given two natural numbers a and c, we say that c is a divisor of a if there exists $q \in \mathbb{N}^*$ such that $a = q \times c$ (i.e. if in the division $a \div c$ the remainder is 0).

  $c \mid a$ means that c is a divisor of a.

  Examples:

  * $2 \mid 14$ because $14 = 7 \times 2$.
  * $7 \mid 91$ because $91 = 13 \times 7$.

* If c is not a divisor of a, we write $c \nmid a$.

  Examples:

  * $2 \nmid 15$ because $15 = 7 \times 2 + 1$.
  * $7 \nmid 95$ because $95 = 13 \times 7 + 4$.

* The number 0 and divisibility:

  $2 \mid 0$? $\quad$ $0 \mid 3$?

* Multiples and divisors

  If $c \mid a$, we also say that a is a multiple of c.

  Examples:

  - $2 \mid 14 \quad \rightarrow \quad 14$ is a multiple of 2.
  - $7 \mid 91 \quad \rightarrow \quad 91$ is a multiple of 7.

* The set of numbers that are multiples of c is denoted by $\dot{c}$.

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

Divisibility

* Exercise: find all divisors of number 20.
* For every natural number n, 1 and n are allways divisors of n. The rest of divisors are called proper divisors.
* Def: A natural number $p > 1$ is called a prime number if it does not have proper divisors (i.e., its only divisors are 1 and p).
* There is a good reason to exclude $p = 1$ from the set of prime numbers (we will go to that shortly.

  An alternative definition where we do not have to single out $p = 1$:

  Def: A natural number is prime if it has exactly two divisors.
* If a number is not a prime number, we say that it is a composite number.

Prime numbers: basic questions

* Is n a prime numbers?

  a) Is 97 a prime number?

  b) Is 883 a prime number?

  When can we stop looking for divisors?

* Find all prime numbers smaller than n:
  Eratostenes sieve.
  http://www.visnos.com/demos/sieve-of-eratosthenes

* Exercice: Adapt Eratostenes sieve to find all prime number bigger than 170 and smaller than 200.

Descomposition into prime factors (Factorization)

* It is not difficult to convince ourselves that every number can be writthen as a product of prime numbers.

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

364	2
182	2
91	7
13	13
1	

Traditional algorithm (in Spain)

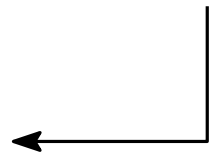
* Prime numbers are the "bricks" from which the rest of the numbers are made up.

  We will see that express a number as a product of primes (factorice the number) gives a lot of information.

Descomposition into prime factors (Factorization)

* Fundamental Theorem of Arithmetic:
  Every natural number can be written as a product of prime numbers. Furthermore, the decomposition is unique.

  for this to be true we need to exclude 1 from the set of prime numbers



* First part (all numbers can be factorized) is easy to show:
  If n is prime, we are done.
  If n is not prime, it has a divisor a, and we have that $n = a \cdot b$. Now, we repeat the argument with a and b.

  To show that the decomposition is unique (not counting the order, of course) is not that easy, and we will not go into that.

Prime factors and divisors

* Exercice: Find all divisors of 60 and compare the factorization of 60 and the factorizations of its divisors.

* In general:

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

$2 \times 7 \times 7 \times 19 = 1862$ is a divisor of $245\,784$

* Decomposing a number into prime factors gives all the information about its divisorss.

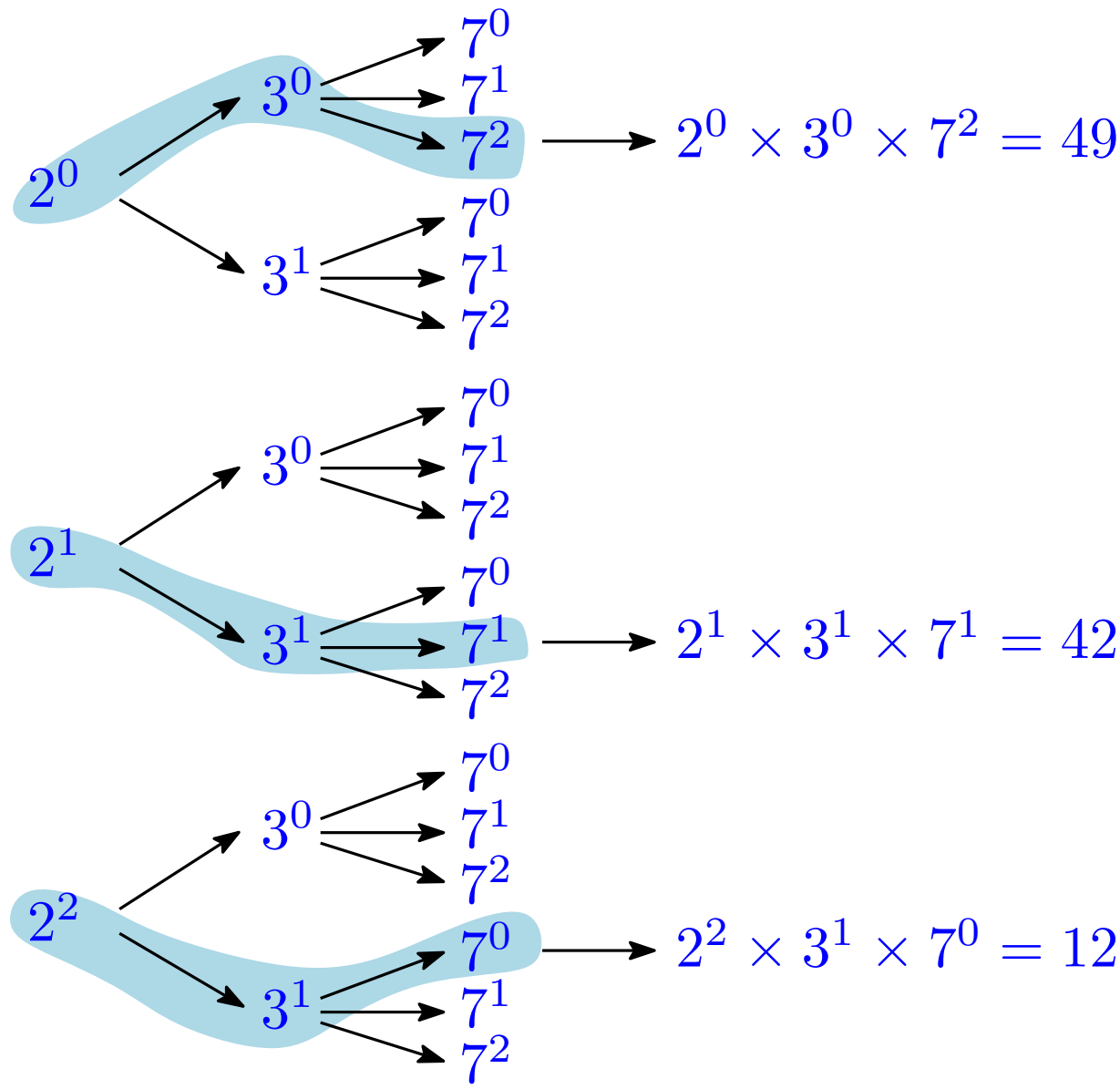
  A good way of seeing that is to arrange the divisors into a tree.

Prime factors and divisors

* Example:

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

  Tree with the divisors.



Prime factors and divisors

* Using this tree we can answer a lot of questions: (observe that sometimes it is not necessary to construct the whole tree)

  1. How many divisors does the number have?
  2. How may divisors are even/odd/multiples of ...?
  3. Find the divisors that are multiples of 28.

* The best way of checking that you understand this is to answer this exercice:

  Knowing that $5720 = 2^3 \times 5 \times 11 \times 13$,

  1. how may divisors does the number 5720 have?
  2. find all odd divisors of 5720.
  3. how many divisors of 5720 are multiples of 22?

Counting the number of divisors

* Observe that we have found the following formula for the number of divisors:

  If $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k}$ then n has

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

  (If you have understood previous slide, it is not necessary to memorice this formula).

Backwards reasoning

* A good way of improving conceptual understanding is to use backwards reasoning.

  We have seen how, given the factorization, we can answer questions about the divisors.
  In the following examples we will need to reason backwards: starting from properties of divisors, we will have to find the number (its factorization).

1. Find four 3-digit numbers having 20 divisors.
2. Find a number having 30 divisors and such that 20 of them are even numbers.
3. Find the smallest number having 8 divisors.

More applications of factorization

* Find the smallest number for which 140 has to be multiplied in order to get a perfect square.

* Find the smallest number for which 360 has to be multiplied in order to get a perfect cube.

* Let us consider $n = 181405$. Knowing that $181405 = 71 \cdot 73 \cdot 35$, find the product $n = a \cdot b$ $(a, b \in \mathbb{N}, a > b)$ such that $a - b$ is minimum.

Back to a basic question

* Theorem (Euclides, $\sim$ 300 bC):

  There are infinitely many primes.

* Proof:

  Assume the number is finite. Then, we can make a list with all of them:

  $L = \{p_1, p_2, \ldots, p_n\}$ is the list of all prime numbers.

  Consider $q = p_1 \times p_2 \times \cdots \times p_n + 1$.

  1. q is not prime (it is not in the list).
  2. q cannot be factorized (none of the numbers in the list is a divisor of q). Impossible!

Some further comments

* Two consecutive odd prime numbers are called twin primes.

  Examples: 3 and 5 are twin primes, 11 and 13 are also twin primes.

* It is unknown whether the number of twin primes is finite.

  The biggest known twins: $p = 65516468355 \cdot 2^{333333} + 1$ and $p + 2$.

  (Sept. 2013)

  ↓

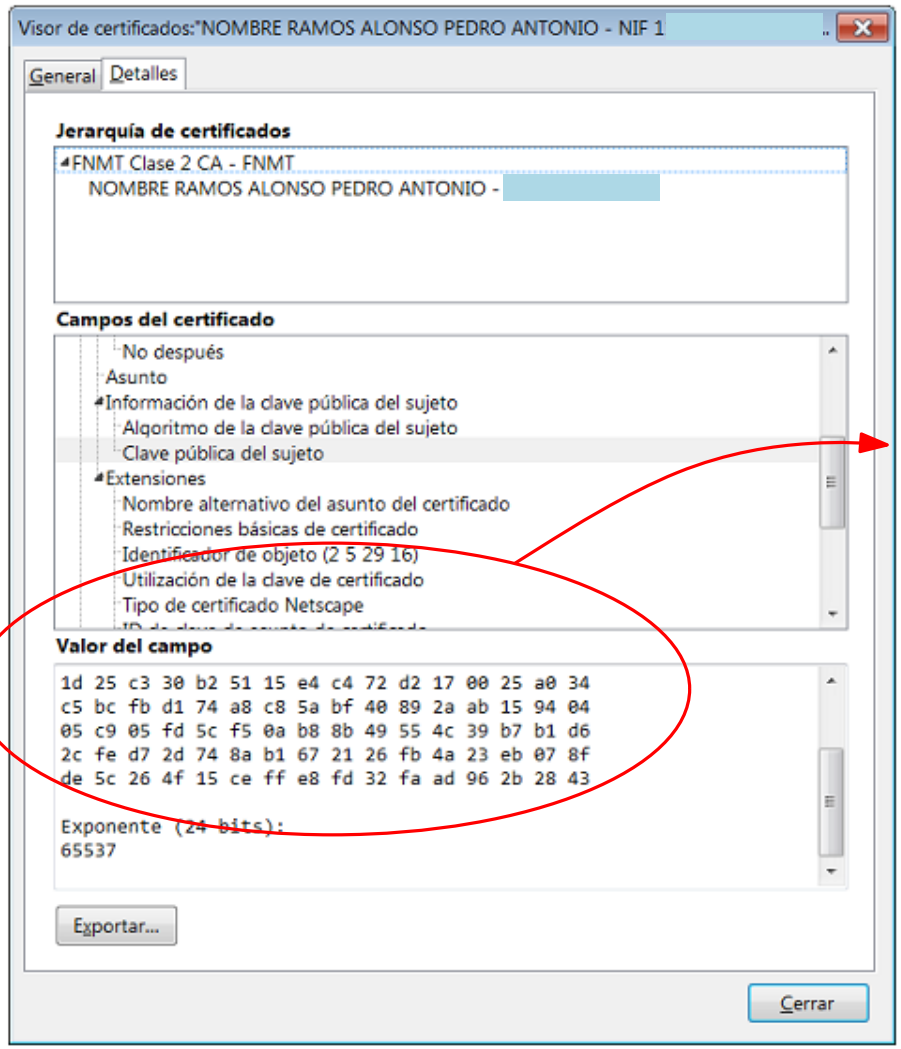
  100355 dígitos

* Biggest known prime number (Sept. 2013) was

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

(12978189 digits).

Any real application?



Security in Internet is mostly based on the fact that it is not known how to factorize big numbers.

RSA: Public key criptography.
Public key in the figure is a number (of about 600 digits in base 10, but it is expressed in hexadecimal form - base 16).

More about this subject:
http://tinyurl.com/pnla4xy

Two properties of divisibility

* If both m and n are even, then $17 \times n + 23 \times m$ is also an even number.

  This property can be generalized as follows.

* If a is a multiple of c, then all multiples of a are also multples of c.

  Equiv: If $c \mid a$ then $c \mid (k \times a)$ (for every k).

* If a and b are multiples of c, then $a + b$ is a multiple of c.

  Equiv: If $c \mid a$ and $c \mid b$, then $c \mid (a + b)$.

* Combining these two properties::

  If a and b are multiples of c, then $k \times a + j \times b$ is alwyas a multiple of c.

  Equiv: If $c \mid a$ and $c \mid b$, then $c \mid (k \times a + j \times b)$.

Greatest common divisor

* Greatest common divisor of numbers a and b, $\gcd(a, b)$, is the biggest natural number that divides both a and b.

* Why learning problems can appear here?

  Maybe because most of the time is not devoted to understanding the concept but to the algorithm for its computation.

* Exercises:

  a) $\gcd(40, 15)$

  b) $\gcd(38478, 1)$

  c) $\gcd(384787, 0)$

Computation of $\gcd(a, b)$

* From the factorization.

  Knowing that

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

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

  find $\gcd(17640, 12474)$.

Let us try to think, and not just remember the "recipe".

* The greatest common divisor of a and b is the product of the common factors in the factorizations of a and b. (With the smallest exponent).

Computation of $\gcd(a, b)$

* Remark: From the factorization of a and b it is also possible to obtain all common divisors of a and b.

  Find all common divisors of 17640 and 12474.

* Using this idea, the following property can be shown:

  The common divisors of a and b are the divisors of $\gcd(a, b)$.

* We have a rectangular room, with sides $6{,}30$ m and $4{,}50$ m. We want to use square tiles to put the floor, and we do not want to break any tile. If we want the tiles to be as big as possible,

  1. what will be the size of the tiles?
  2. how many tiles will we need?

Greatest common divisor of several numbers

* The definition is the same:
  $\gcd(a_1, a_2, \ldots, a_k)$ is the biggest common divisor of $a_1, a_2, \ldots, a_k$.
* The algorithm using factorization is exactly the same:
  If we know that
  $$17640 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$
  $$12474 = 2 \cdot 3^4 \cdot 7 \cdot 11$$
  $$3591 = 3^3 \cdot 7 \cdot 19$$
  $$4998 = 2 \cdot 3 \cdot 7^2 \cdot 17$$
  find $\gcd(17640, 12474, 3591, 4998)$.
* Remark: for more than two numbers it is also true that the common divisors of a set of numbers are the divisors of the greatest commond divisor of the set.

"Mental" calculation of $\gcd$

* It is useful to compute "at a glance" examples like ...

  a) $\gcd(9, 24)$
  b) $\gcd(17, 284)$
  c) $\gcd(8, 68)$

* The following property can be useful:

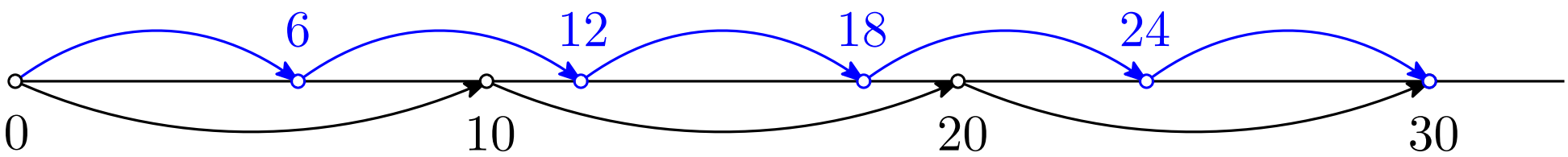
  If k is a common divisor of a and de b, then

$$\gcd(a, b) = k \cdot \gcd(a/k, b/k).$$

* Ex: find $\gcd(84, 24)$.

Least common multiple

* The least common multiple of two natural numbers a and b, denoted $\mathrm{lcm}(a, b)$, is the smallest natural number that is a multiple of both a and b.
* Learning difficulties are similar to the ones we already mentioned about the greatest common divisor.
* Exercises:
  a) $\mathrm{lcm}(6, 10)$
  b) $\mathrm{lcm}(29834, 1)$
* The number line can be a good tool for understanding.



How can we compute the least common multiple?

* In Primary school, just with the definition (mental calculation).
* Divisibility in the curriculum (LOMCE, Madrid, P-6)

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.

* Decomposition into prime factors is not included.

Algorithm to compute $\mathrm{lcm}(a, b)$

* We want to find the least common multiple of $a = 3591$ and $b = 14994$ knowing that

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

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

Let us try to think, and not just remember the "recipe".

* Idea:

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

is a common multiple. Can we find a smaller one?

* Property:,

$$\mathrm{lcm}(a, b) = \frac{a \times b}{\gcd(a, b)}$$

Algorithm to compute $\mathrm{lcm}(a, b)$

* We also have shown that:

  The least common multiple of a and b is the product of all the factors that appear in the factorizatons. Common factors are taken with the biggest exponent.

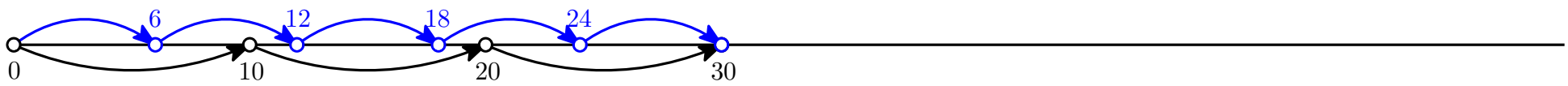
* This algorithm also works to compute the least common multiple of more than two numbers.

  Remark:

  It is not true that $\gcd(a, b, c) \times \mathrm{lcm}(a, b, c)$ equals $a \times b \times c$

A property of the least common multiple

* Common multiples of two or more numbers are the multiples of their least common multiple.



Common multiples of 6 and 10?

* A lighthouse flashes every 16 minutes and a neighbour lighthouse flashes every 12 minutes. We know that both have flashed at midnight and we arrive at 5 pm.

  1. how many times have they flashed simultaneously before we arrived?
  2. what time do we see them to flash simultaneously for the first time?

Divisibility rules

* Arithmetic with remainders. A first example: even/odd.

* Let $r(a, n)$ be the remainder obtained when a is divided by n.

  Question: can we find $r(a + b, n)$ from $r(a, n)$ and $r(b, n)$?

* If $r(a, 3) = 2$ and $r(b, 3) = 2$, how much is $r(a + b, 3)$?

* Using this approach, we are going to deduce divisibility rules (actually, rules to compute remainders) for 3, 4, 5, 6, 8 and 9.

* Remark: no additional visibility rules will be alowed, unless they are properly justified when you use them.