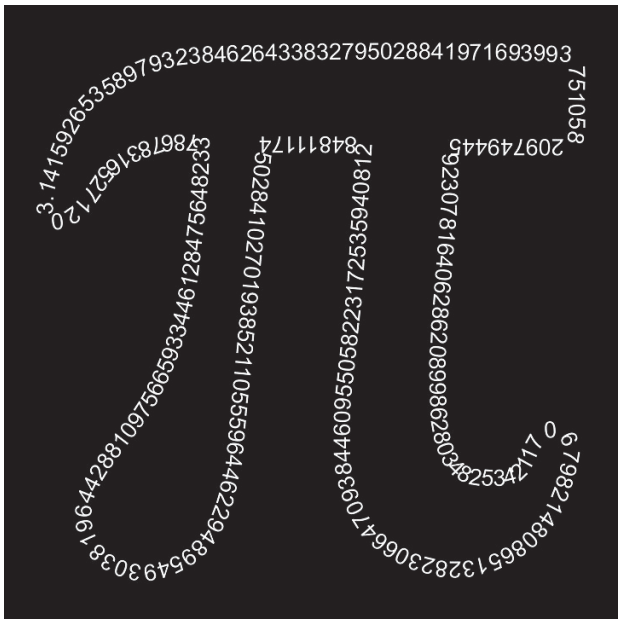
MATHS BASIC COURSE FOR UNDERGRADUATES



Leire Legarreta, Iker Malaina and Luis Martínez

Faculty of Science and Technology

Department of Mathematics

University of the Basque Country

4th SUBJECT: DIVISIBILITY

1 Integer numbers

In Number Theory, one of the basic concepts is the idea of *divisibility*. Thus, the main idea of this subject is the divisibility with remainder of integer numbers.

Definition. *Let $a, b \in \mathbb{Z}$. By definition a is said to be divisible by b, and it is written in the form $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ac$. In that case, it is said that a is a divisor of b, b is a multiple of a or that b can be divided by a. When this relation is not fulfilled, we can express it as $a \nmid b$.*

The following properties are immediate:

Properties. *Let $a, b, c \in \mathbb{Z}$. Then:*

(i) $a \mid b$ *if and only if* $|a| \mid |b|$, *where* $|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}$

(ii) $a \mid 0$ *and* $1 \mid a$

(iii) $a \mid 1$ *if and only if* $a = \pm 1$

(iv) $a \mid a$

(v) *if* $a \mid b$ *and* $b \mid a$, *then* $a = \pm b$

(vi) *if* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$

(vii) *if* $a \mid b$ *and* a *and* b *are both positive integer numbers, then* $a \leq b$

(viii) *if* $a \mid b$ *and* $a \mid c$, *then* $a \mid (bx - cy)$, *for any* $x, y \in \mathbb{Z}$.

2 Division Algorithm

Proposition. *Let a and b be two integer numbers, such that $b \neq 0$. Then there exist two unique integer numbers q and r such that $a = qb + r$, with $0 \leq r < |b|$. In that case, q is called the quotient and r the remainder.*

Proof. *Let us take the rational number $\frac{a}{b}$ (if a and b have opposite signs, the negative sign is associated to a and the proof is carried for $b > 0$). There exists an integer q for which $q \leq \frac{a}{b} < q + 1$. Multiplying the previous expression by b, we obtain $qb \leq a < (q + 1)b$. Hence, $r = a - qb$, and it can be noticed that the previously mentioned properties fullfill.*

Remark. *The next properties are immediate:*

(i) *If $r = 0$, a is divisible by b.*

(ii) *The condition $0 \leq r < |b|$ characterizes the division algorithm. An expression like $21 = (-3)(-5) + 6$ is not a consequence of the division algorithm.*

(iii) *If we fix b, the amount of possible remainders is finite. More precisely, the remainder could be $0, 1, 2, \ldots, |b| - 1$.*

Exercise. *The square of any integer number a has the form $3k$ or $3k + 1$. This is, if we divide a^2 by 3, the remainder will be 0 or 1.*

Proof. *If a is divided by 3, all the possible remainders are 0, 1 or 2. This is, there exist three possibilities:*

(i) *if $a = 3q$, then $a^2 = 9q^2 = 3(3q^2) = 3k$;*

(ii) *if $a = 3q + 1$, then $a^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 = 3k + 1$;*

(iii) *if $a = 3q + 2$, then $a^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1 = 3k + 1$.*

3 Numeral systems

The simplest way to address numbers is the *decimal system*, which uses the digits 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9. For example, 108 is addressed by the following sum:

$$1 \cdot 10^2 + 0 \cdot 10^1 + 8 \cdot 10^0.$$

Remark. *In this subject, we are only going to work with integer numbers, but in general, if the number has a coma, the first digit after the coma is multiplied by 10^{-1}, the second one by 10^{-2}, etc.*

However, there is no reason to restrict always to the decimal system. For example, computers can use octal number systems (multiples of 8), or hexadecimal systems (multiples of 16). In order to perform operations, a computer decomposes the number 108 in powers of two:

$$(E1)108 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0.$$

If we express 108 in powers of 4, we obtain the following:

$$108 = 1 \cdot 4^3 + 2 \cdot 4^2 + 3 \cdot 4^1 + 0 \cdot 4^0,$$

which is addressed by $(1230)_4$. And in base 9:

$$108 = 1 \cdot 9^2 + 3 \cdot 9^1 + 0 \cdot 9^0,$$

this is, $(130)_9$. To obtain these expressions, the division algorithm is used.

Remark. *Notice that:*

$$108 = 3 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 3 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0.$$

A particularity of the first way (E1) to express the number 108*:*

$$108 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$$

is that all coefficients are smaller than 2*.*

Proposition. *Let* $b \geq 2$ *(*$b \in \mathbb{N}$*), which we call base. Any natural number* $n \in \mathbb{N}$ *can be written, in a unique manner, as a combination of powers of* b*:*

$$n = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0,$$

with $0 \leq a_i < b$ *for any* i*, and with* $a_m \neq 0$*. Thus, we can express the number* n *as:* $n = (a_m a_{m-1} \dots a_2 a_1 a_0)_b$*.*

Proof. *The division algorithm has to be applied repeatedly. First,* $n = n_1 b + a_0$*; later* $n_1 = n_2 b + a_1$*, and we follow until we reach an expression like* $n_{m-1} = n_m b + a_{m-1}$*, (being* $a_{m-1} < b$*). Using these expressions and substituting in* $n = n_1 b + a_0$ *we obtain:*

$$n = (((n_m b + a_{m-1} \dots) b + a_2) b + a_1) b + a_0 = n_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0.$$

Exercise. *How can we change from the base* b *to the base* 10*?*

For example, $(3043)_5 = 3 \cdot 5^3 + 0 \cdot 5^2 + 4 \cdot 5 + 3 = 398$.

Exercise. *How can we change from the base* 10 *to the base* b*?*

For example, to express 1025 in the base 7, we divide it by 7 and we get

$$1025 = 146 \cdot 7 + 3.$$

Next, $146 = 20 \cdot 7 + 6$ and $20 = 2 \cdot 7 + 6$. Thus,

$$1025 = 146 \cdot 7 + 3 = (20 \cdot 7 + 6) \cdot 7 + 3 = ((2 \cdot 7 + 6) \cdot 7 + 6) \cdot 7 + 3,$$

and by subtracting the common factors:

$$1025 = 2 \cdot 7^3 + 6 \cdot 7^2 + 6 \cdot 7 + 3 = (2663)_7.$$

Remark. *In the hexadecimal system, we need* 16 *digits. Therefore, to the digits 0, 1, 2, ..., 9, we add the letters A (=10), B (=11), C (=12), D (=13), E (=14) and F (=15).*

Exercise. *How can we change from base* 10 *to base* 16*?*

For example, $3027 = 189 \cdot 16 + 3$ and $189 = 11 \cdot 16 + 13$, and consequently $3027 = (BD3)_{16}$.

Definition. *Let a and b be two integer numbers, such that at least one of them is nonzero. The greatest common divisor of a and b, which is denoted by $gcd(a, b)$, is the unique positive integer number d fulfilling the following properties:*

(i) $d \mid a$ *and* $d \mid b$

(ii) *if* $c \mid a$ *and* $c \mid b$, *then* $c \mid d$.

Exercise. $gcd(-12, 18) = 6$.

The divisors of -12 are ± 1, ± 2, ± 3, ± 4, ± 6 and ± 12, and the divisors of 18 are ± 1, ± 2, ± 3, ± 6 and ± 18.

Remark. *The following properties are fulfilled:*

(i) $gcd(a, b) = gcd(b, a)$;

(ii) $gcd(a, b)$ *exists and it is finite;*

(iii) $gcd(a, b)$ *is always positive. In fact,* $gcd(a, b) = gcd(-a, b) = gcd(a, -b) = gcd(-a, -b) = gcd(|a|, |b|)$;

(iv) $gcd(a, 0) = |a|$.

Proposition. *If a and b are two integer numbers (at least one of them is nonzero), then there exist two numbers x_0 and y_0 for which $gcd(a, b) = ax_0 + by_0$. This last expression is called Bezout's identity.*

Proof. *Let us define the set $C = \{ax + by : ax + by > 0, x, y \in \mathbb{Z}\}$. Clearly $C \subseteq \mathbb{N}$ and C is nonempty (for instance, $a^2 + b^2 \in C$). Since C is an ordered set, let us call its first element d; in other words, there exist $x_0, y_0 \in \mathbb{Z}$ for which $d = ax_0 + by_0$. Now let us see that d is the greatest common divisor of a and b.*

1) Using the division algorithm, we can write $a = qd + r$, being $0 \leq r < d$. Thus,

$$r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0).$$

If $r > 0$, then $r \in C$ and $r < d$, and this is contrary to the definition of d. Therefore, $r = 0$, and consequently $d \mid a$. Analogously, it can be proved that $d \mid b$.

2) If $c \mid a$ and $c \mid b$, we know that c divides any linear combination of a and b, and hence, $c \mid d$.

Remark. *The previous linear combination is not unique. For example,* $3 = gcd(6, 9) = 6 \cdot (-1) + 9 \cdot 1 = 6 \cdot 5 + 9 \cdot (-3)$.

Definition. *If a and b are two nonzero integers, these numbers are called coprimes if they fulfill $gcd(a, b) = 1$.*

Corollary. *Let a and b be two nonzero integer numbers. These numbers are coprimes if and only if there exist $x_0, y_0 \in \mathbb{Z}$ for which $1 = ax_0 + by_0$ is fulfilled.*

Exercise. *If $a \mid bc$ and $gcd(a, b) = 1$, then $a \mid c$.*

Proposition. *If $a = qb + r$, then $gcd(a, b) = gcd(b, r)$.*

Proof. *Let us call $d = gcd(a, b)$. Since r is an integer combination of a and b, it follows that $d \mid r$. In addition to this, d is also the greatest common divisor of b and r. In fact, if there exists c such that $c \mid b$ and $c \mid r$, then $c \mid a$, and consequently $c \mid d$, as we desired.*

Exercise. *Calculate $gcd(1479, 272)$.*

We divide the number 1479 by 272 ($1479 = 5 \cdot 272 + 119$). Thus,

$$\gcd(1479, 272) = \gcd(272, 119).$$

By repeating the same operation, $272 = 2 \cdot 119 + 34$. Hence,

$$\gcd(1479, 272) = \gcd(272, 119) = \gcd(119, 34).$$

Again, $119 = 3 \cdot 34 + 17$, and consequently

$$\gcd(1479, 272) = \gcd(272, 119) = \gcd(119, 34) = \gcd(34, 17).$$

Finally, $34 = 2 \cdot 17 + 0$. Therefore,

$$\gcd(1479, 272) = \gcd(272, 119) = \cdots = \gcd(17, 0) = 17.$$

4 Euclidean algorithm

Let $a, b \in \mathbb{Z}$. Without any loss of generalization, we can assume that these numbers are positive, since $\gcd(a, b) = \gcd(|a|, |b|)$. Suppose that $a \geq b$. Dividing a by b we obtain,

$$a = q_1 b + r_1, \quad \text{where} \quad 0 \leq r_1 < b.$$

We know that $\gcd(a, b) = \gcd(b, r_1)$. If $r_1 = 0$, then $\gcd(a, b) = \gcd(b, r_1) = b$, and we have finished. In the other case, we divide b by r_1:

$$b = q_2 r_1 + r_2, \quad \text{such that} \quad 0 \leq r_2 < r_1.$$

It holds $\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2)$. If $r_2 = 0$, then $\gcd(a,b) = \gcd(r_1,r_2) = r_1$, and we have finished. If not, we divide r_1 by r_2:

$$r_1 = q_3 r_2 + r_3, \quad \text{such that} \quad 0 \leq r_3 < r_2.$$

The process continues until we reach a division by 0, which is achieved by a finite number of divisions, since $r_1 > r_2 > r_3 > \cdots \geq 0$. If the first division with remainder equal to 0 is the $(n+1)$-th division, then

$$r_{n-1} = q_{n+1} r_n + 0,$$

and $\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_{n-1},r_n) = \gcd(r_n,0) = r_n$.

How can we use Euclidean algorithm to achieve Bezout's identity?

$$\begin{aligned}
a &= q_1 b + r_1, \quad \text{such that} \quad 0 \leq r_1 < b \\
b &= q_2 r_1 + r_2, \quad \text{such that} \quad 0 \leq r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, \quad \text{such that} \quad 0 \leq r_3 < r_2 \\
&\cdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, \quad \text{such that} \quad 0 \leq r_{n-1} < r_{n-2} \\
r_{n-2} &= q_n r_{n-1} + r_n, \quad \text{such that} \quad 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0.
\end{aligned}$$

Isolating r_n from the previous equality, we obtain $r_n = r_{n-2} - q_n r_{n-1}$, this is, a linear combination of r_{n-2} and r_{n-1}. From the previous equality, isolating again r_{n-1},

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}, \text{ a linear combination of } r_{n-3} \text{ and } r_{n-2} \text{ is obtained.}$$

Now substituting on the previous expression, r_n is addressed as a linear combination of r_{n-3} and r_{n-2}:

$$r_n = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}).$$

Proceeding in this way, we can address r_n as a linear combination of a and b.

Exercise. *Address gcd*$(1479, 272)$ *as a linear combination of* 1479 *and* 272.

$$\begin{aligned}
1479 &= 5 \cdot 272 + 119, \\
272 &= 2 \cdot 119 + 34, \\
119 &= 3 \cdot 34 + 17,
\end{aligned}$$

$$34 = 2 \cdot 17 + 0.$$

Then, $\gcd(1479, 272) = 17$. And,

$$17 = 119 - 3 \cdot 34 = 119 - 3 \cdot (272 - 2 \cdot 119) =$$

$$7 \cdot 119 - 3 \cdot 272 = 7 \cdot (1479 - 5 \cdot 272) - 3 \cdot 272 = 7 \cdot 1479 - 38 \cdot 272.$$

Proposition. *For any integer number $k \neq 0$, $gcd(ka, kb) = |k|gcd(a, b)$.*

Proof. *If $k > 0$, we have to prove that $gcd(ka, kb) = k.gcd(a, b)$. We have to compare the resulting column of applying Euclidean algorithm to the positive numbers ka and kb with the column obtained by applying the same algorithm to the numbers a and b. The first column is obtained by multiplying the second one by k. In particular, the last nonzero remainder obtained in the first column is the last nonzero remainder obtained in the second column multiplied by k.*
On the other hand, if $k < 0$, we have to prove that $gcd(ka, kb) = -k.gcd(a, b)$. However,

$$gcd(ka, kb) = gcd(|k|a, |k|b) = |k|gcd(a, b) = -k.gcd(a, b).$$

Corollary. *If $gcd(a, b) = d$, then $a = da'$ and $b = db'$, such that $gcd(a', b') = 1$.*

There exists another concept similar to the greatest common divisor of two numbers.

Definition. *If a and b are two nonzero integer numbers, the least common multiple of a and b, which is denoted by $lcm(a, b)$, is the unique integer number m satisfying the following two properties:*

(i) *$a \mid m$ and $b \mid m$*

(ii) *if $a \mid c$ and $b \mid c$, then $m \mid c$.*

Remark. *The following properties are fulfilled:*

(i) *$lcm(a, b) = lcm(b, a)$;*

(ii) *$lcm(a, b)$ always exists;*

(iii) *$lcm(a, b)$ is always positive. In fact, $lcm(a, b) = lcm(-a, b) = lcm(a, -b) = lcm(-a, -b) = lcm(|a|, |b|)$.*

Proposition. *If a and b are two integers, then $gcd(a, b) \cdot lcm(a, b) = |ab|$.*

Proof. *If $a = 0$ or $b = 0$ the result is trivial. In other case, since $gcd(a, b)$ and $lcm(a, b)$ are always positive, we can suppose that $a > 0$ and $b > 0$. Let us denote $d = gcd(a, b)$.*

Then $a = da'$ and $b = db'$ (a' and b' are coprimes). Let us call $m = \frac{ab}{d}$. We have to prove that $m = lcm(a, b)$.

i) m is a multiple of a, since $m = ab'$, and also a multiple of b, since $m = a'b$.

ii) If $c > 0$ is a common multiple of a and b, there exist two integer numbers r and s for which $c = ar = bs$. Now, by Bezout's identity, there exist two integer numbers x_0, y_0 such that $d = ax_0 + by_0$. Dividing c by $m = \frac{ab}{d}$, we obtain the following:

$$\frac{c}{m} = \frac{cd}{md} = \frac{cd}{ab} = \frac{c(ax_0 + by_0)}{ab} = \frac{c}{b}x_0 + \frac{c}{a}y_0 = sx_0 + ry_0,$$

which is in fact an integer number. Hence, $m \mid c$.

5 Prime numbers and Sieve of Eratosthenes

Definition. *An integer number $p > 1$ is said to be prime if its only positive divisors are 1 and p. On the contrary, the number is said to be composed.*

Remark. *The following properties are fulfilled:*

(i) *Any integer number n accepts 1 and n as divisors,*

(ii) *1 is not prime,*

(iii) *2 is the smallest prime, and the only one that is even,*

(iv) *a prime number p cannot be decomposed as $p = ab$ with $1 < a < p$ and $1 < b < p$,*

(v) *if p is a prime number and a is any integer number, then*

$$gcd(a, p) = \begin{cases} p & \text{if } p \mid a \\ 1 & \text{if } p \nmid a \end{cases}$$

Proposition. *If p is a prime and a and b are two integer numbers such that $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. *If $p \nmid a$, then $gcd(a, p) = 1$. And consequently, $p \mid b$.*

Remark. *The previous result only happens for prime numbers. For instance, $6 \mid 2 \cdot 3$, but $6 \nmid 2$ and $6 \nmid 3$.*

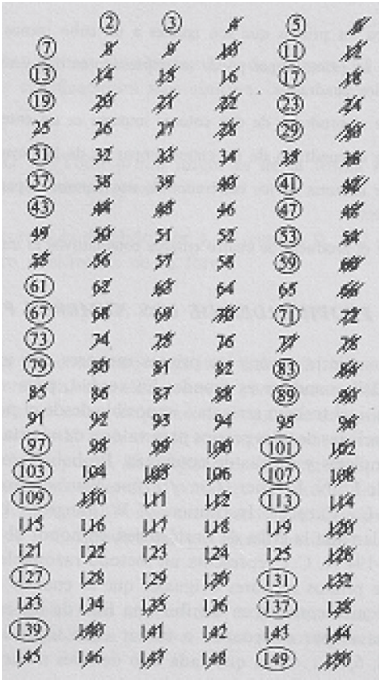
Corollary. Pythagorean Theorem. *$\sqrt{2}$ is an irrational number.*

Proof. *By way of contradiction, if we suppose that $\sqrt{2}$ is a rational number, then it would be of the type $\sqrt{2} = \frac{a}{b}$, being a and b integer numbers and $b > 0$. If it was necessary, simplifying the fraction, let us suppose that a and b are coprimes. Raising to the power of two, we have that $2b^2 = a^2$, and consequently $2 \mid a^2 = aa$. Now, since 2 is prime, we obtain that $2 \mid a$. In other words, there exists an integer number r for which $a = 2r$. Substituting, we get $2b^2 = a^2 = 4r^2$, this is, $b^2 = 2r^2$, and then, $2 \mid b$, which is a contradiction, since a and b are coprime numbers.*

Corollary. *If p is a prime, $a_1, \ldots, a_n$ are integer numbers and $p \mid a_1 \ldots a_n$, then $p \mid a_i$, for some $i \in \{1, \ldots, n\}$.*

Corollary. *If p is a prime and for the prime numbers $p_1, \ldots, p_n$ the following statement $p \mid p_1 \ldots p_n$ is fulfilled, then p, must be one of the factors $p_1, \ldots, p_n$.*

When the natural number (integer and positive) n is big, finding all the primes smaller or equal to it is a difficult problem. The *Sieve of Eratosthenes* addresses a method to find all the prime numbers that are smaller or equal to n, when n is small.
First we write all the integers between 2 and n; then, we erase all the even numbers after 2 (this is, we erase the multiples of 2); then, we erase all the multiples of 3 greater 3, since they are not primes. In this second round, we erase again certain numbers that were already erased. Next, we do the same process with any number after 5 which is a multiple of 5. The process is finished when we erase all the multiples of the prime number p, being $p \leq \sqrt{n}$.
Thus, the remaining numbers are all the primes that are smaller or equal to the initial number n.



6 Fundamental theorem of arithmetic

Theorem. *Any integer number $n > 1$ can be written as a product of certain prime numbers. In addition, this decomposition is unique, except for the order of its factors.*

Proof. *i)* **Existence of the factorization.** *Suppose that S is the set of the integer numbers that cannot be written as a product of prime numbers bigger than 1. By way of contradiction, let us suppose that S is not empty, and denote as a the first element of the set S. By construction, a cannot be a prime (a non composed) number: otherwise, it could not be in S. Thus, $a = mn$, being $1 < m < a$ and $1 < n < a$. Besides, since a is the smallest element of S, $m \notin S$ and $n \notin S$. This is, m and n can be expressed as a product of prime numbers; say $m = p_1 p_2 \dots p_r$ and $n = q_1 q_2 \dots q_s$. Then, $a = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$ is indeed a product of primes, which is a contradiction. Hence, $S = \emptyset$.*

2) **Uniqueness except for the order.** *Suppose that n can be factorized as two different expressions: $n = p_1 p_2 \dots p_r$ and $n = q_1 q_2 \dots q_s$, and that in each case, the primes are ordered decreasingly: $p_1 \leq p_2 \leq \dots \leq p_r$ and $q_1 \leq q_2 \leq \dots \leq q_s$. We have to prove that $r = s$, and that for each index $p_i = q_i$.*

Since $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$, it follows that p_1 divides $q_1 q_2 \dots q_s$, and consequently $p_1 = q_k$, for some k. Specifically, $p_1 \geq q_1$. Analogously, since q_1 divides $p_1 p_2 \dots p_r$, we deduce that $q_1 = p_i$ for a certain i, and in particular, $q_1 \geq p_1$. There-

fore, $p_1 = q_1$.
Now by eliminating the previous factor in the factorization of n*, we obtain* $p_2 \dots p_r = q_2 \dots q_s$*. Repeating the same reasoning, we obtain that* $p_2 = q_2$*. Thus,* $p_3 \dots p_r = q_3 \dots q_s$.
If we assume that $r < s$*, then by doing the successive eliminations, we would obtain* $1 = q_{r+1}q_{r+2} \dots q_s$*, and we get a contradiction, since all the primes of the factorization are bigger than* 1.

Remark. *If* $n < -1$*, since* $-n > 1$*, we have the factorization* $-n = p_1p_2 \dots p_r$*, and then,* $n = -p_1p_2 \dots p_r$.
Besides, in this kind of factorizations, prime numbers can appear repeated, and if we group together these repeated primes, we obtain the canonical factorization of the integer number n.

Theorem. *Any integer* $n \neq 0, \pm 1$ *can be addressed in a single form, as follows:*

$$n = \pm p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$

being $p_1 < p_2 < \dots < p_r$ *prime numbers and the indexes* $k_i > 0$.

Proposition. *If* $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$*, where* $p_1 < p_2 < \dots < p_r$ *are primes, all the indexes* k_i *are positive, and* $m \mid n$*, then* $m = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}$*, where* $h_i \leq k_i$*, for any value of* i.

Proof. *If* $m \mid n$*, then* $n = cm$*, being* c *an integer. By taking the factorization of the integer numbers in prime numbers, we have that* $m = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$ *and* $c = r_1^{l_1} r_2^{l_2} \dots r_t^{l_t}$. *Then,*

$$p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s} r_1^{l_1} r_2^{l_2} \dots r_t^{l_t}.$$

Now from the Fundamental theorem of arithmetic, we know that the prime numbers and the powers of them that appear in both sides of the equation must be equal. Hence, in particular, each q_j *must be equal to some* p_i*, and its power* $h_j \leq k_i$.

Finally, we finish this subject saying that this previous factorization technique can be applied to calculate the greatest common divisor and the least common multiple of two integer numbers, avoiding the use of the Euclidean algorithm (although the Euclidean algorithm is numerically more efficient), as follows:

Proposition. *If* $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ *and* $m = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}$*, where* $p_1 < p_2 < \dots < p_r$ *are prime numbers and* $k_i, h_i \geq 0$*, for any index, then*

(i) $gcd(m, n) = p_1^{\min(k_1,h_1)} p_2^{\min(k_2,h_2)} \dots p_r^{\min(k_r,h_r)}$;

(ii) $lcm(m, n) = p_1^{\max(k_1,h_1)} p_2^{\max(k_2,h_2)} \dots p_r^{\max(k_r,h_r)}$;

(iii) $mn = lcm(m, n) \cdot gcd(m, n)$.