The fractions exploration and simplification

by Fabienne Chaplais

Table of Content

1. Introduction

2. Division and Fractions

We discover here how the fractions of integers are related to the division of integers.

2.1 The euclidian division in the integers set $\mathbb{Z}$

Theorem 1

Assume $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ *are integers such as* $b > 0$.

Then there exists a unique couple of integers $(q, r) \in \mathbb{Z} \times \mathbb{N}^*$ *such as:*

- $a = bq + r$,
- *and* $0 \leq r \leq b - 1$.

Definition

Assume $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ *are integers such as* $b > 0$.

Then the unique couple of integers $(q, r) \in \mathbb{Z} \times \mathbb{N}^*$ *such as:*

- $a = bq + r$,
- *and* $0 \leq r \leq b - 1$.

is composed of the quotient q *and the remainder* r *of the euclidian division of* a *by* b.

Notation

Assume $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ *are integers such as* $b > 0$.

Assume q *and* r *are respectively the quotient and the remainder of the euclidian division of* a *by* b.

Then this is denoted $a \div b = q$, *remains* r.

Proof of theorem 1

Assume $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ are integers such as $b > 0$.

<u>Existence of the couple $(q, r) \in \mathbb{Z} \times \mathbb{N}^*$ that fulfils the conditions</u>:

If $0 \leq a \leq b - 1$, then $q = 0$ and $r = a$ fulfil the conditions.

Assume $a \geq b$, and define the sequence $(r_k, k \geq 0)$ by the recursive property:

- r_0=a,
- r_{k+1}=r_k-b.

Then the sequence is strictly decreasing in $\mathbb{Z}$, so that there exists only a finite number of indexes $k \geq 0$ such as $r_k \geq 0$.

Let's denote k^0 the last index such as $r_k \geq 0$, and let's define $q = k^0$, and $r = r_{k^0}$.

Then $r = a - qb$, and $r - b < 0$, so that $r \leq b - 1$.

Consequently, $a = bq + r$, and $0 \leq r \leq b - 1$.

Assume now $a < 0$, so that $a' = - a$ is such as $pa'0$.

Let's define $(q', r') \in \mathbb{Z} \times \mathbb{N}^*$ the couple such as $a' = bq' + r'$ and $0 \leq r' \leq b - 1$.

If $r' = 0$, then $a' = q'b$, so that $a = - a' = (-q')b = qb + r$, with $q = - q'$, and $r = 0$.

Let's assume now the $r' > 0$.

Then $a = - a' = b(-q') - r' = b(-q' - 1) + (b - r') = bq + r$, with $q = - q' - 1$ and $r = b - r'$.

It remains to prove that $0 \leq r \leq b - 1$.

But $r' > 0$, such as $b - r' < b$, that is $r \leq b - 1$.

And $r' \leq b - 1$, so that $b - r' \geq 1$, that implies $r \geq 0$.

QED

2.2 Fractions of integers

Definition 2

Assume $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ *are integers such as* $b \neq 0$.

Then the fraction $\dfrac{a}{b}$ *is the unique quantity such as* $b \times \dfrac{a}{b} = a$.

The integer a is the numerator of the fraction $\dfrac{a}{b}$*, and the non-zero integer b is its denominator.*

Theorem 2

Assume $(a, b) \in \mathbb{Z}^2$ *are integers of any sign.*

Then the fraction $\dfrac{a}{b}$ *is equal to the integer* 0 *if and only if* $a = 0$.

Proof

Assume $(a, b) \in \mathbb{Z}^2$ are integers of any sign.

If $a = 0$, then the fraction $\dfrac{a}{b}$ is equal to the integer 0, because $b \times 0 = 0$.

Assume now that the fraction $\dfrac{a}{b}$ is equal to the integer 0.

Then $a = 0$, because $b \times 0 = 0$.

Theorem 3

For any integer $a \in \mathbb{Z}$*, the fraction* $\dfrac{a}{1}$ *is equal to the integer* a.

Proof

For any integer $a \in \mathbb{Z}$, $1 \times a = a$.

Definition 3

Assume $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ *are integers such as* $b \neq 0$.

Then a is a multiple of b (or b is a divider of a) if there exists a non-zero integer $k \in \mathbb{Z}^*$ *such as* $a = kb$.

Theorem 4

Assume $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ *are integers such as* $b \neq 0$ *and* a *is a multiple of* b.

Then the non-zero integer $k \in \mathbb{Z}^*$ *such as* $a = kb$ *is unique*.

Proof

Assume $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ are integers such as $b \neq 0$ and a is a multiple of b.

Assume $(k_1, k_2) \in \mathbb{Z} \times \mathbb{Z}^*$ are integers such as $a = k_1 b$ and $a = k_2 b$.

Then $(k_1 - k_2)b = k_1 b - k_2 b = a - a = 0$, and $b \neq 0$.

Consequently $k_1 = k_2$.

QED

Theorem 5

Assume $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ *are integers such as* $b \neq 0$ *and* a *is a multiple of* b. *Then the fraction* $\frac{a}{b}$ *is equal to the integer* k *such as* $a = kb$.

Corollary 1

Any integer has an infinity of representations as fractions.

Proof of the corollary 1

Assume $k \in \mathbb{Z}$ is any integer.

For any non-zero integer $b \in \mathbb{Z}^*$, $\frac{kb}{b} = k$ because of theorem 5.

Proof of the theorem 5

Assume $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ are integers such as $b \neq 0$ and a is a multiple of b.

Let's consider the integer $k \in \mathbb{Z}$ such as $a = kb$. Then, by definition of the fraction $\frac{a}{b}$, is is equal to the integer k.

3.1 The non-negative decimal numbers and the powers of 10

Definition 4

A decimal number is a number x *for which there exist natural integers* $(X, N) \in \mathbb{N}^2$ *such as* $x = \frac{X}{10^N}$.

Notation

For any natural $(X, N) \in \mathbb{N} \times \mathbb{N}^*$ *with* $N > 0$*, given the decimal expansion of X* $X = X_K X_{K-1} \ldots X_N X_{N-1} \ldots X_0$*, the decimal number* $x = \dfrac{X}{10^N}$ *is denoted with a decimal point between* X_N *and* X_{N-1}*:* $x = X_K X_{K-1} \ldots X_N \bullet X_{N-1} \ldots X_0$.

The integer $E[x] = X_K X_{K-1} \ldots X_N$ *is called the entire part of x, and the sequence of the N last digits* $X_{N-1} \ldots X_0$ *of X is called the decimal part of x.*

Proposition 1

In the particular case where $N = 0$ *and* $X \in \mathbb{N}$ *any natural integer, the decimal number* $x = \dfrac{X}{10^N}$ *is the integer X.*

Proof

For any natural integer $X \in \mathbb{N}$, $\dfrac{X}{10^N} = \dfrac{X}{10^0} = \dfrac{X}{1}$, that is the integer X because of the theorem 1.

3.2 The representations of the decimal numbers

Theorem 6

For any decimal number $x = \dfrac{X}{10^N}$*, with* $(X, N) \in \mathbb{N}^2$*, and for any* $M \in \mathbb{N}$ *such as* $M > N$*, another representation of x is* $x = \dfrac{Y}{10^M}$*, where Y is the natural integer equal to X filled with* $M - N$ *zeroes to the left.*

Corollary 2

For any decimal representation of a decimal number x with a decimal point, you may add as many additional zeroes to the left of the decimal part of x.

In the particular case where x is an integer, you may add a decimal point, and as may zeroes as you wish after it.

Proof of Corollary 2

Assume $(X, N) \in \mathbb{N}^2$ are two natural integers, and assume $M \in \mathbb{N}$ is a natural integer such as $M > N$.

If $N > 0$, the decimal part of $x = \dfrac{X}{10^N}$ is the sequence of the N last digits.

And if we add $M - N$ zeroes to the left of X to obtain Y, the decimal part of $y = \frac{Y}{10^M}$ is the M last digits of Y, that are the decimal part of X plus $M - N$ zeroes to the left.

And because of theorem 2, the decimal number y and x are equal to each other.

If $N = 0, x = \frac{X}{10^N}$ has no decimal part.

And if we add $M - N = M$ zeroes to the left of X to obtain Y, the decimal part of $y = \frac{Y}{10^M}$ is the M last digits of Y, that are composed of M zeroes to the left.

And because of theorem 2, the decimal number y and x are equal to each other.

QED

Proof of theorem 6

Assume $(X, N) \in \mathbb{N}^2$ are two natural integers, and assume $M \in \mathbb{N}$ is a natural integer such as $M > N$.

If Y is the natural integer equal to X filled with $M - N$ zeroes to the left, then it is the product $Y = 10^{M-N}X$ of X and 10^{M-N}.

Moreover, 10^M is the product $10^M = 10^{M-N} \times 10^N$ of 10^N by 10^{M-N}.

But we shall see in § 4.2 below, that if we multiply the numerator and denominator of a fraction by a same quantity, the resulting fraction is equal to the initial fraction.

Consequently, the decimal numbers $x = \frac{X}{10^N}$ and $y = \frac{Y}{10^M}$ are equal.

QED

4. Equality of fractions

4.1 The Signs Rules for fractions

Definition 6

Assume $x \in \mathbb{Z}$ is an integer of any sign.

Then the absolute value $|x|$ of x is define as, depending on the sign of x:

- *If $x = 0$, then $|x| = 0$.*
- *If $x > 0$, the $|x| = x$.*
- *If $x < 0$, then $|x| = -x$, the positive opposite of x.*

Definition 7

Assume $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ are integers such as $b \neq 0$. Then the following signs rules apply:

- *If $a = 0$, then $\frac{a}{b}$ is the integer 0.*
- *If $a > 0$ and $b > 0$ or $a < 0$ and $b < 0$, then $\frac{a}{b} = \frac{|a]}{|b|} > 0$.*
- *If $a < 0$ and $b > 0$, or $a > 0$ and $b < 0$, then $\frac{a}{b} = -\frac{|a]}{|b|} < 0$.*

Theorem 7

The definition 5 is consistent with the signs rules for the multiplication in $\mathbb{Z}$, and with the theorems 2 and 3.

As a matter of fact, the definition 5 generalises the signs rules in $\mathbb{Z}$.

Proof

Assume $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ are integers such as $b \neq 0$.

1) $a = 0$:

As $0 = 0 \times b$, then, because of theorem 3, $\frac{a}{b}$ is the integer 0.

2) $b = 1$ and $a \neq 0$:

Then, because of theorem 3, $\frac{a}{b}$ is the integer a, being of the same sign than a.

Namely, $\frac{a}{b} = \frac{|a]}{|b|} > 0$ when $a > 0$ (and $b = 1 > 0$), and $\frac{a}{b} = -\frac{|a]}{|b|} < 0$ when $a < 0$ (and $b = 1 > 0$).

Consequently, the definition 5 is consistent with the theorem 1.

3) a is a multiple of b and $a \neq 0$:

Assume $k \in \mathbb{N}$ is the natural integer such as $a = kb$. $k \neq 0$ because $a \neq 0$ and 0 is absorbent for the multiplication in $\mathbb{Z}$.

Then, because of theorem 4, $\frac{a}{b}$ is the non-zero integer k.

But because of the signs rules in $\mathbb{Z}$:

- If $k > 0$, then either $a > 0$ and $b > 0$ or $a < 0$ and $b < 0$. This is consistent with the fact that is those cases, $\frac{a}{b} = \frac{|a]}{|b|} > 0$.
- And if $k < 0$, then either $a > 0$ and $b < 0$ or $a < 0$ and $b > 0$. This is consistent with the fact that is those cases, $\frac{a}{b} = -\frac{|a]}{|b|} < 0$.

Consequently, the definition 5 is consistent with the signs rules in $\mathbb{Z}$ and with the theorem 2.

QED

4.2 The cross product rule

Theorem 8

Assume $(a, b, c, d) \in \mathbb{Z}^4$ are non-zero integers such as $b \neq 0$ and $d \neq 0$.

Then the fractions $\frac{a}{b}$ and $\frac{c}{d}$ are equal if and only if $ad = bc$.

Corollary 3

Assume $(a, b, c) \in \mathbb{Z}^3$ are integers such as $b \neq 0$.

Then the fraction $\frac{a}{b}$ is equal to the integer c if and only if $a = bc$.

Proof of corollary 3

Because of theorem 2, the integer c is equal to the fraction $\frac{c}{1}$.

Consequently, because of theorem 6, the fraction $\frac{a}{b}$ is equal to the integer c if and only if $a \times 1 = bc$, with $a \times 1 = a$.

QED

Proof of theorem 8

Assume $(a, b, c, d) \in \mathbb{Z}^4$ are non-zero integers such as $b \neq 0$ and $d \neq 0$.

Assume $\frac{a}{b} = \frac{c}{d}$.

Then, by definition 2, $b \times \frac{a}{b} = a$, so that $bd \times \frac{a}{b} = ad$. And $d \times \frac{c}{d} = c$, so that $bd \times \frac{c}{d} = bc$.

Consequently, as $\frac{a}{b} = \frac{c}{d}$, $ad = bc$.

Assume now $ad = bc$.

But the fraction $\frac{a}{b}$ is such as $b \times \frac{a}{b} = a$, and the fraction $\frac{c}{d}$ is such as $d \times \frac{c}{d} = c$.

Then $bc \times \frac{a}{b} = ac$ and $ad \times \frac{c}{d} = ac$.

Consequently, because $bc = ad$, $\frac{a}{b} = \frac{c}{d} = \frac{ac}{bc}$.

QED

4.3 The multiplicative rule for fractions

Theorem 9

Assume $(a, b, k) \in \mathbb{Z} \times \mathbb{Z}^* \times \mathbb{Z}^*$ *are integers such as* $b \neq 0$ *and* $k \neq 0$.

Then the fraction $\frac{ka}{kb}$ *is equal to the fraction* $\frac{a}{b}$.

Corollary 4

Any fraction has an infinity of "representations" (all the fractions that are equal to it).

The corollary 4 is a direct consequence of the theorem 6.

Proof of theorem 9

Assume $(a, b, k) \in \mathbb{Z} \times \mathbb{Z}^* \times \mathbb{Z}^*$ are integers such as $b \neq 0$ and $k \neq 0$.

Then, because of the commutativity and associativity of the multiplication in $\mathbb{Z}$, $(ka)b = (kb)a$ so that, because of theorem 8, $\frac{ka}{kb} = \frac{a}{b}$.

QED

5. Simplify fractions down to there canonical form

5.1 Simplification with the Signs Rules

Theorem 8

Assume $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ are integers of any signs such as $b \neq 0$.

Then we may simplify the fraction the following way, depending on the signs of and :

1. *If $a = 0$, then $\frac{a}{b} = 0$, whatever the sign of b.*
2. *If $a = p$, with $p > 0$ and $b = q$ with $q > 0$, then $\frac{a}{b} = \frac{p}{q}$ (> 0).*
3. *If $a = p$, with $p > 0$ and $b = -q$ with $q > 0$, then $\frac{a}{b} = -\frac{p}{q}$ (< 0).*
4. *If $a = -p$, with $p > 0$ and $b = q$ with $q > 0$, then $\frac{a}{b} = -\frac{p}{q}$ (< 0).*
5. *If $a = -p$, with $p > 0$ and $b = -q$ with $q > 0$, then $\frac{a}{b} = \frac{p}{q}$ (> 0).*

The theorem 8 is a rewording of the definition 6, together with the definition 5 of the absolute value.

A consequence of theorem 8 is that the fraction of non-zero integers are all equal to either a fraction of positive integers, of the opposite of such a fraction.

Thus we may simplify further the only fractions of positive integers.

5.2 Further Simplification of Fractions of Positive Integers

Theorem 9

Assume $(p, q) \in (\mathbb{N}^*)^2$ *are positive integers.*

Assume there exists a positive integer $k \in \mathbb{N}^* - \{1\}$*, that is a non-one common divider of* p *and* q*, with* $(p', q') \in (\mathbb{N}^*)^2$ *being such as* $p = kp'$ *and* $q = kq'$*.*

Then $\dfrac{p}{q} = \dfrac{p'}{q'}$*, with* $p' < p$ *and* $q' < q$*.*

Proof

Because of theorem 8, and as $p = kp'$ and $q = kq'$, the fractions $\dfrac{p}{q}$ and $\dfrac{p'}{q'}$ are equal.

Moreover, as $k \neq 1$, and k is a positive integer, then $k \geq 2$.

Consequently, $p \geq 2p' > p'$, and $q \geq 2q' > q'$.

QED

5.3 Down to the Canonical Form

Definition 7

A fraction of positive integers $\dfrac{p}{q}$*, with* $(p, q) \in (\mathbb{N}^*)^2$*, is said to be irreducible if and only if it can not be simplified.*

Theorem 10

For any couple of positive integers $(p, q) \in (\mathbb{N}^*)^2$*, the fraction* $\dfrac{p}{q}$ *is irreducible if and only if* p *and* q *are mutually prime.*

The theorem 10 is a direct consequence of the theorem 9 and of the definition B.2 in appendix B.

Theorem 11

For any fraction of positive integers, there is an only irreducible fraction of positive integers that is equal to it.

That theorem is proved in Appendix A.

Definition 8

The canonical form of a fraction of positive integers is based on its unique irreducible representation: it is the irreducible representation unless the denominator of the latter is equal to 1*, in which case the canonical form is the numerator of that irreducible representation.*

Theorem 12

The successive simplifications of a fraction of positive integers ends with its canonical form.

Proof

The simplification of a fraction of positive integers is a strictly decreasing process fo both its numerator and denominator.

Consequently, as each pair "numerator and denominator" are pairs of positive integers, they both decrease by at least 1 at each simplification process, and they keep minored by 1.

So that the iterative simplifications ends in a finite numbers of steps.

And the final state is the canonical form, because it can not be simplified further.

QED

Theorem 13

Assume $(p, q, k) \in (\mathbb{N}^*)^3$ *are positive integers such as* $k = GCD(a, b)$*, following definition B.3 of the appendix B.*

Then, if $p' = p \div k$ *and* $q' = p \div k$*, with the notation of definition B.4 in appendix B, the canonical form of the fraction* $\dfrac{p}{q}$ *is the fraction* $\dfrac{p'}{q'}$*, unless* $q' = 1$*, in which case its canonical form is the integer* 1*.*

That theorem is a direct consequence of theorem B.4 and definition 8.

Here is the Python code to calculate the numerator and denominator of the canonical form of a fraction of positive integer, given by its numerator and denominator (the function “Euclid” is defined by the Python code at the end of appendix B):

```
def simplify(num,den):
   gcd=Euclid(num, den)
   num=num//gcd
   den=den//gcd
   if den==1:
      return(num)
   else:
       return (num,den)
```

Appendix A

Proof of Theorem 11

A.1 The Fundamental Theorem of Arithmetics

Definition A.1

A non-one positive integer $p \in \mathbb{N}^* - \{1\}$ *is said to be a prime number if it has no other divider except* 1.

Lemma A.1

Assume $p \in \mathbb{N}^*$ *is any positive integer.*

Then either p is a prime number, of p has a prime factor $k \in \mathbb{N}^*$ *(k is a prime number and a divider of p).*

Theorem A.1 (Fundamental theorem of Arithmetics)

Assume $p \in \mathbb{N}^* - \{1\}$ *is any non-one positive integer.*

Then there exists a unique sequence of prime numbers$(k_1, k_2, \ldots, k_n) \in (\mathbb{N}^* - \{1\})^n$ *and a unique sequence of positive integers* $(m_1, m_2, \ldots, m_n) \in (\mathbb{N}^*)^n$ *such as:*

- *if* $n \geq 2$, $k_1 < k_2 < \ldots < k_n$,
- *and* $p = k_1^{m_1} k_2^{m_2} \ldots k_n^{m_n}$

Definition A.2

The prime numbers $(k_1, k_2, \ldots, k_n) \in (\mathbb{N}^* - \{1\})^n$ *defined in theorem A.1 are called the prime factors of p, with the respective multiplicities the positive integers* $(m_1, m_2, \ldots, m_n) \in (\mathbb{N}^*)^n$.

The formula $p = k_1^{m_1} k_2^{m_2} \ldots k_n^{m_n}$ *is called the prime numbers decomposition of the positive integer* p.

Proof of Lemma A.1

Let's prove the result by recursion on $p \geq 2$.

Initialisation: $p = 2$

$p = 2$ is a prime number, because if $k \in \mathbb{N}^* - 1$ is a non-one divider of 2, then k is an integer such as $1 < k \leq 2$, and thus $k = 2$.

Recursion:

Hypothesis: For some $p \geq 2$, the result is fulfilled for any integer q such as $2 \leq q \leq p$.

Let's denote $p^+ = p + 1$, and let's prove the result for p^+.

If p^+ is a prime number, the result is obvious.

Assume then p^+ is a not a prime number, and let's denote k a divider of p^+ that is neither equal to 1 nor to p^+.

Then k is an integer such as $1 < k < p^+$, so that $2 \leq k \leq p$.

Then, because of the hypothesis of recursion, either k is a prime number, and thus it is a prime factor of p^+, or it has a prime factor k'.

In the last case, let's denote p' the positive integer such as $p^+ = kp'$, and k'' the positive integer such as $k = k'k''$.

Then $p^+ = (k'k'')p' = k'(k''p')$ because of the associativity of the multiplication.

Consequently, k' is a prime factor of p^+.

QED

Proof of theorem A.1

Let's prove the existence of the decomposition of a non-one positive integer $p \in \mathbb{N}^* - \{1\}$ in prime factors par recursion on $p \geq 2$.

The proof of the uniqueness of such a decomposition is rather complicated, and we shall admit it.

Initialisation: $p = 2$

As 2 is a prime number, the result in fulfilled with $n = 1$, $k_1 = 2$ and $m_1 = 1$: $p = 2^1$.

Recursion:

Hypothesis: For some $p \geq 2$, the result is fulfilled for any integer q such as $2 \leq q \leq p$.

Let's denote $p^+ = p + 1$, and let's prove the result for p^+.

If p^+ is a prime number, the result is fulfilled with $n = 1, k_1 = p^+ \textit{ and } m_1 = 1$.

Assume then p^+ is a not a prime number, and let's denote k_1 the smaller prime factor of p^+.

Assume p' is the non-one positive integer such as $p^+ = k_1 p'$, with $2 \leq p' \leq p$.

Then, because of the hypothesis of recursion, there exists $(k'_1, k'_2, \ldots, k'_{n'}) \in (\mathbb{N}^* - \{1\})^{n'}$ and a unique sequence of positive integers $(m'_1, m'_2, \ldots, m'_{n'}) \in (\mathbb{N}^*)^{n'}$ such as:

- if $n' \geq 2, k'_1 < k'_2 < \ldots < k'_{n'}$,
- and $p' = {k'_1}^{m'_1} {k'_2}^{m_2} \ldots {k'_{n'}}^{m'_{n'}}$

Moreover, as k_1 is the smaller prime factor of p^+, $k_1 \leq k'_1$.

If $k_1 < k'_1$, then the result is fulfilled for p^+ with $n = n' + 1$, $(k_2, \ldots, k_n) = (k'_1, k'_2, \ldots, k'_{n'})$, $m_1 = 1$, and $(m_2, \ldots, m_n) = (m'_1, m'_2, \ldots, m'_{n'})$

If $k_1 = k'_1$, then the result is fulfilled for $p^+$with $n = n'$, $(k_1, k_2, \ldots, k_n) = (k'_1, k'_2, \ldots, k'_n)$, $m_1 = m'_1 + 1$, and $(m_2, \ldots, m_n) = (m'_2, \ldots, m'_n)$.

This ends the proof of the existence of a decomposition into prime factors of any non-one positive integer.

A.2 Proof of Theorem 11

Lemma A.2

Assume $(p, q) \in (\mathbb{N}^*)^2$ *are positive integers.*

Then p and q are mutually prime if and only if at least one of the following conditions is true:

1. $p = 1$,
2. $q = 1$,
3. $p \neq 1, q \neq 1$ *and they share no prime factor.*

Proof

If $p = 1$ and/or $q = 1$, as 1 has no divider except itself, p and q are mutually prime.

If $p \neq 1, q \neq 1$ and they are mutually prime, then they share no divider except 1, that is not a prime number. Consequently, they share no rime factor.

Assume now $p \neq 1, q \neq 1$ and they share no prime factor, and let's prove that they are mutually prime.

Indeed, if they were not mutually prime, they would have a common factor $k \neq 1$.

But because of lemma A.1, k is either a prime number, and thus a common prime factor of p and q, or it would have a prime factor k', that would be a common prime factor of p and q.

This is in contradiction with the hypothesis that they don't share any prime factor.

Hence they are mutually prime.

QED

Appendix B

The Greater Common Divider of Integers

B.1. The common dividers of Two Positive Integers

Definition B.1

Assume $(a, b, k) \in (\mathbb{N}^*)^3$ *are positive integers.*

Then k is a common divider of a and b if there exist positive integers $(a', b') \in (\mathbb{N}^*)^2$ *such as* $a = ka'$ *and* $b = kb'$.

Proposition B.1

1 *is a common divider of any two positive integers.*

Proof

Assume $(a, b) \in (\mathbb{N}^*)^2$ are positive integers.

Then 1 is a common divider of a and b, because $a = 1 \times a$ and $b = 1 \times b$.

B.2 Mutually Prime Positive Integers

Definition B.2

Assume $(a, b) \in (\mathbb{N}^*)^2$ *are positive integers.*

Then a and b are mutually prime if and only if they don't share any common divider except 1.

B.3 The GCD of two Positive Integers

Theorem B.2

The common dividers of two positive integers $(a, b) \in (\mathbb{N}^*)^2$ *have a unique common divider* k *that is greater or equal to all the common dividers of* a *and* b.

Definition B.3

The Greater Common Divider of two positive integers $(a, b) \in (\mathbb{N}^*)^2$*, is the positive integer* $k = GCD(a, b)$ *such as:*

- k *is a common divider of* a *and* b*,*
- *and no common divider of* a *and* b *is strictly greater than* k.

Proof of theorem B.2

Assume $(a, b) \in (\mathbb{N}^*)^2$ are positive integers, and assume $(k_1, k_2) \in (\mathbb{N}^*)^2$ are common dividers of a and b such as, for any common divider $k \in \mathbb{N}^*$, $k_1 \geq k$ and $k_2 \geq k$.

Then $k_1 \geq k_2$ and $k_2 \geq k_1$, so that $k_1 = k_2$.

QED

Theorem B.3

Two positive integers $(a, b) \in (\mathbb{N}^*)^2$ *are mutually prime if and only if there greater common divider if equal to* 1

Definition B.4

Assume $(a, b) \in (\mathbb{N}^*)^2$ *are positive integers such as* b *is a divider of* a.

Then "a divided by b" is the positive integer $k = a \div b$ *such as* $a = kb$.

Note that it is the quotient of the euclidian division of a by b, the rest being equal to 0.

Theorem B.4

Assume $(a, b) \in (\mathbb{N}^*)^2$ *are positive integers, and assume* $k \in \mathbb{N}^*$ *is the greater common divider of* a *and* b*. Then* $a' = a \div k$ *and* $b' = b \div k$ *are mutually prime.*

Proof

Assume $(a, b) \in (\mathbb{N}^*)^2$ are positive integers, and assume $k = GCD(a, b)$.

Denote $a' = a \div k, b' = b \div k$, and $k' = GCD(a', b')$.

Denote $a'' = a' \div k'$ and $b'' = b' \div k'$.

Then $a = ka' = k(k'a'') = (kk')a''$ and $a = kb' = k(k'b'') = (kk')b''$, so that kk' is a common divider of a and b.

Hence $kk' \leq k$ by definition of the greater common divider.

But $kk' \geq k$, with equality if and only if $k' = 1$, so that a' and b' are mutually prime (cf. theorem B.3).

B.4 The euclidian algorithm to calculate the GCD

Theorem B.5

Assume $(a, b) \in (\mathbb{N}^*)^2$ are positive integers, and assume $a' = b$ and b' is the remainder of the euclidian division of a by b.

Then either $b' = 0$ and $a' = GCD(a, b)$, or $GCD(a', b') = GCD(a, b)$.

Proof

Assume $(a, b) \in (\mathbb{N}^*)^2$ are positive integers, and assume $a' = b$ and b' is the rest of the euclidian division of a by b.

Assume first $b' = 0$.

Then b is a divider if a, so that it is a common divider if a and b (because $b = 1 \times b$).

If k is a common divider of a and b, then it is a divider of b, so that $k \leq b$.

Consequently, $b = GCD(a, b)$.

Assume now $b' \neq 0$, so that a' and b' are positive integers.

Denote $k = GCD(a, b)$ and $k' = GCD(a', b')$, and let's prove $k = k'$.

Denote q the quotient of the euclidian division of a by b.

Then, because b' is the remainder of that division, $a = qb + b'$ (and $b = a'$, so that $a = qa' + b'$).

Denote $(a'', b'') \in (\mathbb{N}^*)^2$ the positive integers such as $a' = k'a''$ and $b' = k'b''$.

Then $a = k'(qa'' + b'')$, and $b = k'a''$, so that k' is a common divider of a and b, and $k' \leq k$.

On the other hand, $a' = b$ and $b' = a - qb$.

So that, if we denote $(a''', b''') \in (\mathbb{N}^*)^2$ he positive integers such as $a = ka'''$ and $b = kb'''$, $a' = kb'''$ and $b' = k(a''' - qb''')$.

Consequently, k is a common divider of a' and b', and $k \leq k'$.

As a conclusion $k' \leq k$ and $k \leq k'$, so that $k = k'$.

QED

The euclidian algorithm

Initialisation:

Acquire two positive integers a and b.

Preprocessing:

If $a < b$, exchange a and b:

Memorise a in the intermediate variable $a1$.

Replace a by b.

Replace b by $a1$.

Processing (with $a \geq b$):

While $b > 0$

Memorise a in the intermediate variable $a0$.

Replace a by b.

Replace b by the remainder of the euclidian division of $a0$ by b..

(at the end of the conditional loop, $b = 0$): output a.

Theorem B.6

The euclidian algorithm calculate the GCD of the input variables a and b in a finite, les or equal than the initial b, of the conditional loop.

Proof

1) The number of steps is finite and less or equal than the initial b:

As the remainder r of an integer D by an integer $d \leq D$ is between 0 and $d - 1$, each step of the algorithm results in a decreasing of at least 1 of the variable b, that keeps minored by 0.

So after at most b steps, the variable b becomes equal to 0.

2) The final value of a is the GCD of the initial values of a and b:

Because of the preprocessing, we may assume $a \geq b$.

And because of theorem B.5, each step of the conditional loop lets the GCD of a and b unchanged.

The final value of a goes with a value of b equal to zero.

Consequently, because of theorem B.5 again, it is the GCD of the previous values of a and b, that is equal to the GCD of the initial values of a and b.

QED

Python code for the euclidian algorithm

```
def Euclid(a,b):
   if a<b:
      a1=a
      a=b
      b=a1
   while b>0:
      a0=a
      a=b
      b=a0%b
   return a
```