The 10 FUNDAMENTAL THEOREMS of ARITHMETIC

1. **[Linear Combination]** If $d \mid a$ and $d \mid b$ then $d \mid w = au + bv$ $(u \in \mathbb{Z},\ v \in \mathbb{Z})$

$$\left\{ \begin{array}{c} d \mid a \\ d \mid b \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} a = d.a' \\ b = d.b' \end{array} \right\} \Rightarrow au + bv = da'u + db'v = d(a'u + b'v) \Rightarrow d \mid (au + bv)$$

---

2. If $d \mid a$ and $d \mid b$ and $a = b.q + r$ $(0 \le r < b)$ then $d \mid b$ and $d \mid r$

$$\left\{ \begin{array}{c} d \mid a \\ d \mid b \\ a = bq + r \\ (0 \le r < b) \end{array} \right\} \Rightarrow \{r = a.1 + b.(-q)\} \Rightarrow r \text{ is a linear combination of a and b } \Rightarrow \left\{ \begin{array}{c} d \mid r \\ d \mid b \end{array} \right\}$$

---

3. **[EUCLID algorithm to find the GCD]** The **GCD** of a and b is the **LAST NON ZERO REST** of all Euclidian Divisions of a by b (rest r_1) ; b by r_1 (rest r_2) ; r_1 by r_2 (rest r_3) , … with $b > r_1 > r_2 > \ldots > r_n \ge 0$

$$\left\{ \begin{array}{c} d \mid a \\ d \mid b \\ a = bq + r_1 \\ 0 \le r_1 < b \end{array} \right\} \Rightarrow \left\{ \begin{array}{c} d \mid b \\ d \mid r_1 \\ b = r_1 q_1 + r_2 \\ 0 \le r_2 < r_1 < b \end{array} \right\} \Rightarrow \left\{ \begin{array}{c} d \mid r_1 \\ d \mid r_2 \\ r_1 = r_2 q_2 + r_3 \\ 0 \le r_3 < r_2 < r_1 < b \end{array} \right\} \Rightarrow \ldots \Rightarrow \left\{ \begin{array}{c} d \mid r_{n-2} \\ d \mid r_{n-1} \\ r_{n-2} = r_{n-1} q_{n-1} + r_n \\ 0 \le r_n < r_{n-1} < \ldots < r_3 < r_2 < r_1 < b \end{array} \right\} \Rightarrow \left\{ \begin{array}{c} d \mid r_{n-1} \\ d \mid r_n \\ r_{n-1} = r_n q_n + 0 \\ 0 \le r_n < r_{n-1} < \ldots < r_3 < r_2 < r_1 < b \end{array} \right\}$$

r_n is the last Rest $\neq 0$, then any common divisor d of a and b is a divisor of r_n

then if $d = GCD(a;b)$ *then* $d \mid r_n \therefore d \le r_n$

But $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-1}q_{n-1} + r_n = r_{n-2} \Rightarrow \{r_n \mid r_{n-1}$ *and* $r_n \mid r_{n-2}\} \Rightarrow r_n \mid r_{n-2}q_{n-2} + r_{n-1} = r_{n-3} \Rightarrow \{r_n \mid r_{n-2}$ *and* $r_n \mid r_{n-3}\} \Rightarrow \ldots \Rightarrow \{r_n \mid r_1$ *and* $r_n \mid b\} \Rightarrow \{r_n \mid b$ *and* $r_n \mid a\}$. *then* $r_n \le d$ *because d was supposed to be the GCD of a and b , eventually we have :*

$r_n \le d$ ***and*** $d \le r_n \Rightarrow d = r_n$. Hence **the last non zero rest** of the divisions **is** the **GCD(*a;b*).**

---

4. **[BÉZOUT fundamental theorem] GCD(*a* ; *b*) = 1 *if* (⇐), *and only if* (⇒) there are two Integers *u* and *v* such that $au + bv = 1$**

a. **Demo of the sufficient condition *(⇐) :***

IF $au + bv = 1$ then any common divisor/factor d of a and b is a divisor/factor of **$au + bv = 1$,** therefore if **$au + bv = 1$** then **GCD(a;b) = 1** *(because the only divisor of 1 is 1)*

b. **Demo of the necessary condition *(⇒) :***

IF GCD(*a* ; *b*) = 1, there must be two integers u and v such that ***au + bv = 1.***

Let's consider the set E^+ of all positive numbers in the form of ***au + bv.*** In that set, there is a **smallest** element : $m = au_0 + bv_0$. *(m > 0)* .Then let's prove that m is a ***divisor*** of both a and b *(in that case m = 1)*

Let's divide a *by* m : $a = mq + r$ *with* $0 \le r < m$.

Then by replacing m by $au_0 + bv_0$ *we get* $a = (au_0 + bv_0)q + r$

$\Leftrightarrow r = a(1 - u_0 q) + b(-v_0 q)$. *Hence* $r = aU + b V$, then r is an element of the set E^+, therefore r must be larger than m, but since we had the condition $0 \le r < m$ we must have $r = 0$. Therefore $a = mq$ *i.e.* $m \setminus a$.

In the same way we can prove that $m \setminus b$ therefore m is a ***common divisor*** of a and b which implies that $m = 1$ ***hence*** $au_0 + bv_0 = 1$

---

5. **GCD(*a* ; *b*) = d** if and only if ***d*** is a common divisor of ***a*** and ***b*** and there are 2 Integers ***u*** and ***v*** such that ***au* + *bv* = d**

a. **IF *au* + *bv* = d** then any common divisor ***k*** of ***a*** and ***b*** is a divisor of ***au* + *bv* =*d***
therefore $k \le d$. If **D** is the ***greatest* common divisor** of a and b then $D \le d$
and ***if d is a common divisor of a and b*** then $d \le D$ therefore ***d* = *D*.**

b. If **GCD(a;b) = d** then ***a* = *d a'*** and ***b* = *db'*** with **GCD(*a'*,*b'*) = 1 (see Th. 6)** then *from Bezout Theorem* (#4)
there are two intergers ***u*** and ***v*** such that ***a'u*+*b'v* = *1*.** Then by multiplying by ***d*** : ***da'u* + *db'v* = *d* ⇔ *au* + *bv* = *d***

---

6. If **GCD (*a* ; *b*) = *d*** and ***a* = *da'*** and ***b* = *db'*** then **GCD (*a'*;*b'*) = 1.**

Demo : If ***k*** is a common divisor of ***a'*** and ***b'*** then ***a' =ka" and b' =kb"*** *(k ≥ 1)*

Then ***a* = *dka"*** and **b = dk b"** ⇒ ***dk*** is a common divisor of ***a*** & **b** ⇒ $dk \le d \Rightarrow k = 1$

---

7. **[GAUSS Fundamental theorem**] : If **GCD(*a* ; *b*) = 1** and ***a*** | ***bc*** then ***a*** | ***c***

$$\begin{Bmatrix} GCD(a\ ;\ b)\ =\ 1 \\ a\ |\ bc \end{Bmatrix} \Leftrightarrow \begin{Bmatrix} au+bv=1 \\ bc=ka \end{Bmatrix} \Rightarrow \begin{Bmatrix} acu+bcv=c \\ bc=ka \end{Bmatrix}$$

$$\Rightarrow acu+kav=c \Rightarrow a(cu+kv)=c \Leftrightarrow a\,|\,c$$

---

8. If **GCD** (*a* ; *b*) = 1 and ***a*** | ***N*** and ***b*** | ***N*** then ***ab*** | ***N***

$$\begin{Bmatrix} GCD(a;b)\ =\ 1 \\ a\,|\,N \\ b\,|\,N \end{Bmatrix} \Leftrightarrow \begin{Bmatrix} GCD(a;b)\ =\ 1 \\ a\,|\,N \\ N=k_2b \end{Bmatrix} \Rightarrow \begin{Bmatrix} GCD(a;b)\ =\ 1 \\ a\,|\,k_2b \\ N=k_2b \end{Bmatrix} \Rightarrow \begin{Bmatrix} a\,|\,k_2 \\ a\,|\,k_2b \\ N=k_2b \end{Bmatrix} \Rightarrow \begin{Bmatrix} k_2=ak_3 \\ a\,|\,k_2b \\ N=k_2b \end{Bmatrix} \Rightarrow N=(ak_3)b=(ab)k_3 \Rightarrow (ab)\,|\,N$$

---

9. If ***m*** = **LCM (*a*;*b*)** and ***d*** = **GCD (*a*;*b*)** then ***md* = *ab***

Let ***M*** be a common multiple of ***a*** and ***b*** then $M = a.k_1$ and $M = b.k_2$, ;

a* = *d.a' and ***b* = *d.b'*** with **GCD(a';b') = 1** then $ak_1 = bk_2 \Leftrightarrow da'k_1 = db'k_2$

$\Leftrightarrow a'k_1 = b'k_2$ *but from* *Gauss Theorem* ***a'*** | k_2 ***and b'*** | k_1 ***then*** $k_2 = a'a"$ ***and*** $k_1 = b'b"$

Therfore ***M* = *ab'b"* = *ba'a"* ⇔ *M*=*da'b'a"*=*da'b'b"* (*a"*=*b"*),** which means that any common multiple of ***a*** and ***b*** is a multiple of ***(da'b')*.**

Reciprocally, any mutliple of ***da'b'*** is a multiple of ***a* = *a'd*** and of ***b* = *b'd*.**

Then all common multiple of ***a*** and ***b*** are in the form ***(a'b'd).k*.**

Hence the Least Common Multiple of ***a*** and ***b*** is exactly ***(a'b'd).1*** . Hence ***m* = *a'b'd* ⇔ *md* = *a'd b'd* ⇔ *md* = *ab*.**

---

10. If ***N*** is a **Prime number** and ***N*** | ***ab*** then ***N*** | ***a*** or ***N*** | ***b***

From the Gauss theorem again, we have ***N*** | ***ab*** *and either* ***GCD(N,b)= 1*** *then* ***N*** | ***a***,
or ***N*** | ***b*** (and we may also have ***N*** | ***a***).
