The 10 FUNDAMENTAL THEOREMS of ARITHMETIC

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

---

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

---

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 $b > r_1, > r_2 > \ldots > r_n \geq 0$

---

4. **[BEZOUT fundamental theorem ()]**

   GCD(a ; b) = 1 if and only if there are two Integers u and v such that $\boldsymbol{au + bv = 1}$

---

5. **GCD(a ; b) = d** if and only if there are two Integers u and v such that $au + bv = d$

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

7. **GAUSS Fundamental theorem** : If **GCD**(a ; b) = 1 and $a \mid bc$ then $a \mid c$

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

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

10. If N is a **Prime number** and $N \mid ab$ then $N \mid a$ or $N \mid b$