Prime Numbers

Definition : ———————————————————————————————

We say p *is prime if* p *is only divisible by* ± 1 *and* $\pm p$

Property

for any integer $a > 1$, *it exist a prime* p *for which* $p|a$

Proof :

lets assume that the negative proposition is true, meaning that it exist $a > 1$, *for any prime* p, p *can't divid* a, *so* a *it self isn't prime, we take the set of dividor of* a *greater than* 1
$D = \{c|a,\ 1 < c < a\}$, *this set isn't empty because if it is there is no divisor for* a *besid* $\pm a$ *and* ± 1 *wich contradict the fact that* a *cant be divisible by prime so* a *will be prime number, hence* $D \neq \varnothing$, *because* $D \subset \mathbb{N}$, *minimum of* D *exist, we take* $d = minD$, *if we suppose that there is* r *for which* $1 < r < d$ *and* $r|d$ *it imply that* $r|a$ *then* $r \in D$ *and* $r < d$ *which will contradict the fact* d *is minimum, meaning* d *cant have any devidor beside* $\pm d$ *and* ± 1, *so* d *is prime, hence contradiction*

Proprety :

Any integer $a > 1$, *it exist* $p_1, p_2, ..., p_t$ *with* $p_1 \leqslant p_2 \leqslant ... \leqslant p_t \quad a = p_1 \times p_2 \times ... \times p_t$

Proof :

Any integer $a > 1$, *if* a *is prime then the assemption is rigth, let see the other one, if* a *is not we take the set of all prime number* $p > 1$ *that can divid* a, $K_1 = \{p|a, p \text{ is prime with } 1 < p < a\}$
$K_1 \neq \varnothing$ *because for any integer* $a > 1$, *it exist a prime* p *for which* $p|a$ *meaning that* $p < a$ *and* p *divid* a *hence* $p \in K_1$ *implying* $K_1 \neq \varnothing$, *the set* $K \subset \mathbb{N}$ *and any* $p \in K_1$ $p < a$, *so* K_1 *has maximum, let* $p_1 = maxK_1$ *that means it exist* $1 < m_1 < a$ *for which* $a = m_1 p_1$, *we do the same for* m_1 *we have the set* $K_2 = \{p|m_1, p \text{ is prime with } 1 < p < m_1\}$ *the same nonemptiness reason as* K_1, *let* $p_2 = maxK_2$ *that means it exist* $1 < m_2 < m_1$ *for which* $m_1 = m_2 p_2$ *meaning that* $p_2 \leqslant p_1$, p_2 *cant be greater then* p_1 *because* $m_1 < a$ *and* p_1 *is the greatest prime number that divid* a, *so if we continue like this we will have after* n *iteration the following result* $m_n = m_{n+1} p_{n+1}$ *with* $1 < m_n < ... < m_2 < m_1$ *and* $p_{n+1} \leqslant ... \leqslant p_2 \leqslant p_1$, *by the well ordering theorem* $1 < m_n < ... < m_2 < m_1$ *this sequence is decreasing, and it born in the bottom by* 1 *hence this sequence has limit number after* t *iteration because we are in* $\mathbb{N}$, *and we know all* $a > 1$ *has a prime number that divid them, and the limit of the sequence is no exeption so* m_t *must equal* p_t *a prime number, because if not* m_t *is greater then* 1 *and not prime we can find* K_t, m_{t+1} *and* p_{t+1} *which will contradict the fact that* m_t *is the limit, hence* m_t *must be prime finally we can arrenge and replace each* m_k *with its value we will get* $a = p_1 \times p_2 \times ... \times p_t$ *with*
$p_1 \leqslant p_2 \leqslant ... \leqslant p_t$

$Proprety:$
$for\ p\ a\ prime\ number\ if\ p|bc\ then\ p\ divid\ b\ or\ c$

$Proof:$
$if\ p|b\ we\ are\ done,\ else\ it\ means\ gcd(p,b) = 1\ and\ by\ the\ extended\ euclidiant\ algorithm\ we\ will\ have\ some\ x,y \in \mathbb{Z},\ for\ wich\ px + by = 1\ implying\ cxp + cby = c,\ p\ divid\ it\ self\ and\ bc\ hence\ p\ divid\ c$

$Proprety:$
$Any\ integer\ a > 1,\ it\ exist\ p_1, p_2, ..., p_t\ with\ p_1 < p_2 < ... < p_t\ and\ \alpha_i\ is\ a\ positive\ integer$

$$a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_t^{\alpha_t}$$

$Proof:$
$Any\ integer\ a > 1,\ it\ exist\ q_1, q_2, ..., q_n\ with\ q_1 \leqslant q_2 \leqslant ... \leqslant q_n \quad a = q_1 \times q_2 \times ... \times q_n,$
$we\ take\ the\ set\ K_1 = \{p|a, p\ is\ prime\ with\ 1 < p < a\}\ its\ obviously\ nonempty\ because\ a\ is\ the\ product\ of\ prime\ numbers,\ the\ max\ exist\ because\ K_1 \subset \mathbb{N}\ and\ for\ all\ p\ in\ K_1\ p < a,\ let\ take\ p_1 = maxK_1, we\ get\ b_1\ after\ we\ divid\ a\ with\ p_1,\ if\ p_1\ divid\ b_1\ we\ get\ b_2\ we\ will\ repeat\ this\ until\ b_k\ that\ cant\ be\ divid\ by\ p_1,\ so\ we\ get\ two\ resulte\ \alpha_1\ the\ number\ of\ time\ we\ divided\ by\ p_1\ and\ b_k\ a\ number\ that\ doest\ have\ the\ p_1\ primery\ number\ so\ we\ are\ left\ with\ b_k = q_1 \times q_2 \times ... \times q_{n-k}\ know\ we\ have\ another\ composition\ and\ we\ take\ K_2 = K_1 - \{p_1\}\ and\ K_2\ is\ not\ empty\ for\ the\ same\ reason\ as\ K_1,\ K_2 \subset K_1\ meaning\ max\ exist\ we\ take\ p_2 = maxK_2\ and\ because\ p_1 \notin K_2\ and\ K_2 \subset K_1\ with\ p_1 = maxK_1,\ p_2 < p_1\ wich\ means\ that\ p_1 \neq p_2, they\ are\ distinct, we\ repeate\ the\ same\ process\ so\ after\ j\ iteration\ we\ will\ have\ K_j \subset ... \subset K_2 \subset K_1, (p_1, \alpha_1), (p_2, \alpha_2), ..., (p_j, \alpha_j),\ because\ every\ K_{i+1}\ is\ strictly\ includ\ in\ K_i, and\ K_{i+1} = K_i - \{p_i\}\ with\ p_i = maxK_i,\ means\ that\ maxK_{i+1} < maxK_i\ wich\ means\ p_{i+1} < p_i,\ implying\ the\ distinction\ of\ each\ p_i\ with\ p_i \neq p_{i+1}.\ the\ numbers\ are\ finit\ so\ this\ sequence\ can't\ continue\ for\ ever\ the\ set\ K_j\ always\ get\ an\ element\ out\ so\ there\ is\ limit\ t\ for\ which\ K_t = \varnothing,\ in\ other\ word\ K_t = K_1 - \{q_1, ..., q_{t-1}\} = \varnothing\ hence\ we\ will\ have\ the\ following\ (p_1, \alpha_1), (p_2, \alpha_2), ..., (p_j, \alpha_j)\ , ..., (p_{t-1}, \alpha_{t-1})\ so\ we\ can\ rewrite\ a\ as\ the\ product\ of\ each\ of\ p_i\ that\ is\ repeated\ \alpha_i\ times,\ hence\ a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_{t-1}^{\alpha_{t-1}}\ with\ p_1 < p_2 < ... < p_t\ suppose\ we\ can\ write\ a\ two\ diffrent\ ways\ a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_t^{\alpha_t}\ and\ a = q_1^{\beta_1} \times q_2^{\beta_2} \times ... \times q_t^{\beta_t}\ we\ know\ that\ p_i|a\ which\ will\ mean\ that\ there\ is\ a\ q_j^{\beta_j}\ that\ p_i\ divid\ for\ some\ j\ and\ by\ the\ nested\ property\ the\ p_i\ is\ distinct\ in\ a\ so\ q_j = p_i\ we\ repeat\ this\ until\ \alpha_i \leqslant \beta_j,\ in\ the\ other\ way\ q_j|a\ we\ already\ tell\ that\ q_j = p_i\ and\ it\ will\ divided\ for\ some\ i\ so\ we\ reapeted\ until\ \beta_j \leqslant \alpha_i, hence\ \alpha_i = \beta_j$
