Lema (4.4.19)

Sea $a \in \mathbb{Z}$. Si $a>1$, entonces el menor divisor positivo de a, mayor que 1, es un número primo.

Dem:

Sea:

$$A = \{x \in \mathbb{Z} \mid x > 1 \text{ y } x \mid a\}$$

$A \subset \mathbb{P}$, además $A \neq \emptyset$, pues $a \in A$ ya que $a > 1$ y $a \mid a$. Como $\mathbb{P}$ está bien ordenado, entonces tiene elemento mínimo. Sea:

$$p = \min A$$

afirmamos que p es primo.

Si p no es primo, entonces existe $q \in \mathbb{Z}$, en $1 < q < p$, tal que $q \mid p$, entonces $q \mid a$, entonces $q \in A$. $\#_c$, pues $p = \min A$ y $q < p$.

q.e.d.

Teorema (4.4.20)

Si $a \in \mathbb{Z}$ y $a > 1$, entonces a es primo o existen $p_1, \dots, p_{k+1}$ números primos tales que:

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_{k+1}.$$

Además $p_1, \dots, p_{k+1}$ son únicos salvo el orden en que aparecen como factores.

Dem:

Por hipótesis $a > 1$, aplicando el lema anterior, sea p_1 el menor entero mayor a 1 que divide a a. Entonces

$$a = p_1 a_1$$

entonces $a_1 < a$. Si $a_1 = 1$, hemos terminado, $a = p_1$, lo que indica que a es primo.

Si $a_1 > 1$, entonces existe p_2 primo tal que:

$$a_1 = p_2 a_2$$

donde $a_2 < a_1$. Entonces:

$$a = p_1 p_2 a_2$$

Si $a_2 = 1$, entonces existen p_1, p_2 primos tales que $a = p_1 p_2$.

Si $1 < a_2$, Continuamos el proceso, obteniendo:

$$a = p_1 a_1$$
$$a_1 = p_2 a_2$$
$$\vdots$$
$$a_k = p_{k+1} a_{k+1}$$

el proceso termina cuando $a_{k+1} = 1$, lo que siempre ocurre, pues en caso contrario, el conjunto:

$$\{a, a_1, a_2, \dots, a_k, a_{k+1}, \dots\} \subset \mathbb{P}$$

donde $a > a_1 > a_2 > \dots$, no tiene elemento mínimo, contradiciendo que esté bien ordenado. Entonces:

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot p_{k+1}.$$

con $p_1, \dots, p_{k+1}$ primos.

Unicidad.

Si $a = p_1 \cdot \dots \cdot p_n$ y $a = q_1 \cdot \dots \cdot q_m$, $p_1, \dots, p_n$ y $q_1, \dots, q_m$ primos, entonces:

$$q_1 \cdot \dots \cdot q_m = p_1 \cdot \dots \cdot p_n$$

entonces $p_1 | q_i$, para algún $i = 1, 2, \dots, m$. Podemos suponer que $i = 1$, pues la elección de los índices está a nuestro arbitrio. En consecuencia $p_1 = q_1$, y por tanto:

$$p_2 \cdot \dots \cdot p_n = q_1 \cdot \dots \cdot q_m$$

continuando con el proceso, obtenemos que: $p_i = q_i \quad \forall i = 1, 2, \dots, n = m$, pues si $n < m$ o $m > n$, entonces un producto de primos es 1, lo que no puede suceder.

q.e.d.

Def.

Si un número primo aparece α-veces como factor del entero $a > 1$, entonces decimos que p tiene multiplicidad α en a. Si $p_1, p_2, \dots, p_n$ son los diferentes factores primos del entero a, y $\alpha_1, \dots, \alpha_n$ sus multiplicidades, la expresión:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

se llama descomposición canónica de a.

Teorema (4.4.22)

Def.

Sean $a,b\in\mathbb{Z}$ con $a\neq 0$ y $b\neq 0$. Decimos que $m\in\mathbb{Z}$, $m>0$, es mínimo común múltiplo (mcm) de a y b, si:

i) $a|m$ y $b|m$.

ii) Si $c\in\mathbb{Z}$ es tal que $a|c$ y $b|c$, entonces $m|c$.

Notación: para decir que m es el mcm de a y b, escribiremos $m=[a,b]$ ó $m=\text{mcm}\{a,b\}$.

Proposición (4.4.24)

Si $m=[a,b]$, entonces m es único.

Teorema (4.4.25)

Si $a,b\in\mathbb{Z}-\{0\}$, entonces existe $m=[a,b]$.

Dem:

Sea:

$$A=\{x\in\mathbb{Z}\mid x>0,\ a|x \text{ y } b|x\}\subset\mathbb{P}$$

claro que $A\neq\emptyset$, pues $x=|a|\cdot|b|\in A$.

Como $\mathbb{P}$ está bien ordenado, entonces A tiene elemento mínimo. Sea:

$$m=\min A.$$

entonces $m>0$, $a|m$ y $b|m$.

Solo resta probar que si $c\in\mathbb{Z}$ tal que $a|c$ y $b|c$, entonces $m|c$. En efecto, por el algoritmo de la división existen $q,r\in\mathbb{Z}$ tales que:

$$c=mq+r;\ 0\leq r<m$$

entonces:

$$r=c-mq \quad \text{con } 0\leq r<m$$

como $a|c$, $a|m$, $b|c$, $b|m$, entonces $a|c-mq$ y $b|c-mq$. Por tanto $r=0$ o $r\in A$.

Si $r\in A$, entonces $r<m$ $\#_c$. Entonces $r=0$. Así $m|c$.

q.e.d.

Proposición (4.4.26)

Si $a,b \in \mathbb{Z}-\{0\}$, entonces:

$$[a,b]=[|a|,|b|]$$

Def.

Sea $n \in P$, y sean $a_0,a_1,\dots,a_n \in \mathbb{Z}-\{0\}$. Decimos que $m \in \mathbb{Z}, m>0$, es mcm de $a_0,a_1,\dots,a_n$, si:

i) $a_k \mid m \ \forall i=0,1,\dots,n$.

ii) Si $c \in \mathbb{Z}$ es tal que $a_k \mid c \ \forall K=0,1,\dots,n$, entonces $m \mid c$.

Teorema (4.4.28)

Si $m=[a_0,a_1,\dots,a_n]$, entonces m es único.

Teorema (4.4.29)

Si $\forall n \in P$, $a_0,a_1,\dots,a_n \in \mathbb{Z}-\{0\}$, entonces existe:

$$m=[a_0,a_1,\dots,a_n]$$

Teorema (4.4.30) (examen)

Si $a,b \in \mathbb{Z}$ con $a>0$ y $b>0$, entonces:

$$ab=(a,b)\cdot[a,b]$$