El Teorema Fundamental de la Aritmética y sus aplicaciones

Pablo L. De Nápoli

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Álgebra I - Segundo cuatrimestre de 2020

Parte I

Repaso de la clase anterior: Números Primos

Números primos

Definición

Un número $p \in \mathbb{Z}$ se dice primo si es distinto de $0, \pm 1$ y sus únicos divisores son ± 1 y $\pm p$. Un número $n \in \mathbb{Z}$ distinto de $0, \pm 1$ que no es primo se dice compuesto.

Los primeros números primos (positivos, menores que 100) son

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$$

$$47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

- Todo entero $n > 1$, o bien es primo o se puede descomponer como producto de números primos (positivos).
- Existen infinitos números primos.
- Notaremos $\mathbb{P}$ al conjunto de los números primos positivos.

La propiedad fundamental de los números primos

Teorema (lema de Euclides, 4.6.3 en el apunte)

Sea p un primo y sean $a, b \in \mathbb{Z}$. Entonces

$$p|a \cdot b \Rightarrow p|a \vee p|b.$$

Por inducción esto se generaliza a un producto de más números

Teorema

Sea p un primo y sean $a_1, a_2, \ldots a_n \in \mathbb{Z}$. Entonces

$$p|\prod_{k=1}^{n} a_k \Rightarrow p|a_k \text{ para algún } k$$

Parte II

El Teorema fundamental de la aritmética

El Teorema fundamental de la aritmética

Teorema

Cada entero $n \in \mathbb{N}$, $n > 1$ es o bien primo o se escribe como producto de primos. Y esta descomposición es única salvo el orden de los factores.

- La existencia de la factorización ya la probamos en la clase anterior.

Un ejemplo

Para ilustrar el teorema, obtengamos dos factorizaciones del número 360. Un procedimiento posible, es ir dividiendo a 360 por los primos en orden de magnitud, hasta obtener un 1:

360	2
180	2
90	2
45	3
15	3
5	5
1	

Luego obtenemos la factorización:

$$360 = 2 \times 2 \times 2 \times 3 \times 5 \times 5$$

Un ejemplo (2)

¿Qué sucede si hubiéramos empezado dividiendo por otro primo? Por ejemplo por 5:

360	5
72	3
24	3
8	2
4	2
2	2
1	

Esto conduce la factorización:

$$360 = 5 \times 3 \times 3 \times 2 \times 2 \times 2$$

Pero ambas factorizaciones sólo difieren en el orden de los factores, tal como afirma el teorema.

Demostración de la unicidad de la factorización

Hagamos nuevamente inducción completa en n. Para $n = 1$ el teorema no afirma nada.
Sea entonces $n > 1$, y supongamos que el teorema es válido para todo $n' < n$.
Supongamos que n admite dos factorizaciones como producto de primos:

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

siendo los p_i y los q_i primos (eventualmente alguna de las factorizaciones puede constar de un sólo primo).
Tomemos un primo en la factorización de la izquierda, por ejemplo p_1. Por el lema de Euclides, deducimos que $p_1 | q_i$ para algún i. Pero entonces como q_i es primo, $p_1 = q_i$ o $p_i = 1$ (lo que es imposible pues 1 no es primo); es decir que hemos probado que p_1 debe necesariamente aparecer en la factorización de la derecha.

Demostración de la unicidad de la factorización (2)

Podemos entonces. cancelar p_1 en ambos lados de la igualdad obteniendo dos descomposiciones del número $n' = n : p_1$ como producto de primos:

$$n' = p_2 p_3 \dots p_r = q_1 q_2 q_3 \dots q_{i-1} q_{i+1} \dots q_s$$

Notemos que $n' < n$, entonces en virtud de la hipótesis inductiva, las dos descomposiciones de n' sólo pueden diferir en el orden de los factores: es decir que $r = s$ y los números $q_1, q_2, \dots, q_{i-1}, q_{i+1}, \dots q_s$ deben ser los mismos que p_2, p_3, ...p_r, sólo que en otro orden.
Deducimos entonces que las dos descomposiciones supuestas de n sólo difieren en el orden de los factores.
En virtud del principio de inducción completa, hemos demostrado el teorema para todo $n \in \mathbb{N}$.

La factorización en forma estándar (1)

Notemos que en la descomposición dada por el teorema fundamental, los primos pueden repetirse. Por ejemplo

$$360 = 2 \times 2 \times 3 \times 5 \times 2 \times 3$$

Agrupando los primos que se repiten podemos expresar a cada número n como productos de primos diferentes ordenados en forma creciente, elevados a ciertas potencias.

$$360 = 2^3 \times 3^2 \times 5^1$$

Podemos si queremos incluir otros primos que no aparecen en esta factorización con exponente cero, ej:

$$360 = 2^3 \times 3^2 \times 5^1 \times 7^0 \times 11^0$$

Esta forma de escribir la factorización la llamaremos forma estándar.

La factorización en forma estándar (2)

Definición

Si $p \in \mathbb{N}$ es un primo, definimos la valuación p-ádica $v_p : \mathbb{N} \to \mathbb{N}_0$ del siguiente modo: $v_p(n)$ como el exponente del primo p en la factorización de n si p dvide a n, y 0 sino. De esta forma la factorización de $n \in \mathbb{N}$ puede escribirse

$$n = \prod_{p|n} p^{v_p(n)}$$

Claramente la valuación p-ádica está bien definida, en virtud del teorema fundamental de la aritmética.
Más explícitamente podríamos definir v_p como el máximo exponente k tal que p^k divide a n:

$$v_p(n) = \text{máx}\{k \in \mathbb{N}_0 : p^k | n\}$$

En el ejemplo

$$360 = 2^3 \times 3^2 \times 5^1 \times 7^0 \times 11^0$$

$$v_p(360) = \begin{cases} 3 & \text{si} \quad p = 2 \\ 2 & \text{si} \quad p = 3 \\ 1 & \text{si} \quad p = 5 \\ 0 & \text{si} \quad p \neq 2, 3, 5 \end{cases}$$

Una observación útil

A veces nos convendrá escribir simplemente la factorización estándar en la forma:

$$n = \prod_p p^{v_p(n)}$$

donde el producto sobre todos los primos $p \in \mathbb{P}$ es formalmente infinito. Pero en realidad, sólo finitos factores son distintos de 1 (aquellos donde $v_p(n) > 0$, es decir $p|n$). Por lo que

$$\prod_p p^{v_p(n)} = \prod_{p|n} p^{v_p(n)}$$

Propiedades de la valuación p-ádica (1)

Proposición

Sean $a, b \in \mathbb{N}$, entonces para todo primo p,

$$v_p(a \cdot b) = v_p(a) + v_p(b)$$

Demostración.

Si las factorizaciones de a y b son

$$a = \prod_{p \in \mathbb{P}, p|a} p^{v_p(a)}, \quad b = \prod_{p \in \mathbb{P}, p|b} p^{v_p(b)},$$

la de ab es

$$ab = \prod_{p \in \mathbb{P}, p|a \vee p|b} p^{v_p(a)+v_p(b)}.$$

En consecuencia,

$$v_p(ab) = v_p(a) + v_p(b)$$

Propiedades de la valuación p-ádica (2)

Proposición

Sean $a, b \in \mathbb{N}$, *entonces* $a|b$ *si y sólo si*

$$v_p(a) \leq v_p(b) \text{ para todo primo } p \in \mathbb{P}$$

Demostración

- Supongamos primero que $a|b$, entonces existe $c \in \mathbb{N}$ tal que $b = ac$, y por el teorema anterior:

$$v_p(b) = v_p(a) + v_p(c)$$

  Pero $v_p(c) \geq 0$, luego $v_p(a) \leq v_p(b)$, como afirmamos.
- Por otro lado si, $v_p(a) \leq v_p(b)$ para todo primo p y definimos:

$$c = \prod_{p \in \mathbb{P}, p|b} p^{v_p(b) - v_p(a)}$$

  tendremos que $c \in \mathbb{N}$ (pues los exponentes son enteros no negativos) y, razonando como en el teorema anterior, que $ac = b$. En consecuencia, $a|b$.

Propiedades de la valuación p-ádica (3)

Teorema

Sean $a, b \in \mathbb{N}$ y $p \in \mathbb{P}$, entonces Probar que si $a, b \in \mathbb{N}$, entonces:

$$v_p(a+b) \geq \text{mín}(v_p(a), v_p(b)$$

Demostración.

Sea $j = v_p(a)$ y $k = v_p(b)$ Entonces $p^k | a$ y $p^j | b$. Sea $l = \text{mín}(j, k)$. Entonces $p^l | a, p^l | b$ luego $p^l | a + b$ y en consecuencia

$$l \leq v_p(a+b)$$

que es lo que afirmamos. □

Factorización de enteros en $\mathbb{Z}$

El teorema fundamental de la aritmética se puede extender a enteros negativos, simplemente agregando un signo.

Si $a \in \mathbb{Z}$, $a \neq 0$ su factorización en forma estándar es

$$a = \operatorname{sgn}(a) \cdot \prod_{p \in \mathbb{P}, p|a} p^{v_p(a)}$$

donde

$$v_p(a) = v_p(|a|)$$

$$\operatorname{sgn}(a) = \begin{cases} 1 & \text{si} \quad a > 0 \\ -1 & \text{si} \quad a < 0 \end{cases}$$

Parte III

Máximo común divisor y mínimo común múltiplo en términos de la factorización en primos

Máximo común divisor y mínimo común múltiplo en términos de primos

Teorema

Sean $a, b \in \mathbb{N}$, entonces

i) *El máximo comun divisor $(a : b) = mcd(a, b)$ entre ellos se puede escribir*

$$(a : b) = mcd(a, b) = \prod_{p|a \wedge p|b} p^{\text{mín}(v_p(a), v_p(b))}$$

ii) *Similarmente, el mínimo común múltiplo $[a : b] = mcm(a, b)$ entre ellos se puede escribir*

$$[a : b] = mcm(a, b) = \prod_{p|a \vee p|b} p^{\text{máx}(v_p(a), v_p(b))}$$

ii)

$$[a : b] \cdot (a : b) = a \cdot b$$

Ejemplo

360 =2^3 * 3^2 * 5^1

$$v_p(360) = \begin{cases} 3 & \text{si} & p = 2 \\ 2 & \text{si} & p = 3 \\ 1 & \text{si} & p = 5 \\ 0 & \text{para los otros} & p \end{cases}$$

490 =2^1 * 5^1 * 7^2

mcd(360,490) = 10 = 2^1 * 5^1

mcm(360,490) = 17640 = 2^3 * 3^2 * 5^1 * 7^2

Una caracterización del mcd

Lema

Sean $a, b \in \mathbb{N}$. El máximo común divisor $d = (a : b)$ entre a y b está caracterizado por las siguientes propiedades.

i) *Es un divisor común: $d|a$ y $d|b$.*

ii) *Cualquier otro divisor común d' lo divide: si $d'|a$ y $d'|b$, entonces $d'|d$.*

Demostración.

Es claro que d satisface i). Veamos que cumple ii): sabemos que existen $s, t \in \mathbb{Z}$ tales que

$$s \cdot a + t \cdot b = d$$

Entonces si d' es un divisor común de a y b, d' debe dividir a d.
Para ver que i) y ii) caracterizan a d observamos que si $\tilde{d}$ también cumple i) y ii), $d|\tilde{d}$ y $\tilde{d}|d$ por lo que $d = \tilde{d}$. □

Demostración del mcd en términos de primos

Sea

$$d = \prod_{p \in \mathbb{P}} p^{\min(v_p(a), v_p(b))} \in \mathbb{N}$$

Probaremos que d satiface la caracterización del máximo común divisor

i) Es un divisor común: $d|a$ y $d|b$. Para todo primo $p \in \mathbb{P}$:

$$v_p(d) = \min(v_p(a), v_p(b)) \leq v_p(a) \Rightarrow d|a$$

Similarmente:

$$v_p(d) = \min(v_p(a), v_p(b)) \leq v_p(b) \Rightarrow d|b$$

ii) Cualquier otro divisor común d' lo divide: si $d'|a$ y $d'|b$, entonces $d'|d$. Supongamos ahora que d' es otro divisor común: entonces

$$v_p(d') \leq v_p(a), \quad v_p(d') \leq v_p(b)$$

luego para cualquier primo p,

$$v_p(d') \leq \min(v_p(a), v_p(b)) = v_p(d)$$

en consecuencia $d'|d$.

La caracterización del mcm

Lema

Sean $a, b \in \mathbb{N}$. El mínimo común múltiplo $m = mcm(a, b) = [a : b]$ entre a y b está caracterizado por las siguientes propiedades.

i) *Es un múltiplo común: $a|m$ y $b|m$.*

ii) *Cualquier múltiplo m' es divido por él: si $a|m'$ y $b|m'$, entonces $m|m'$.*

Razonando como antes, si definimos

$$m = \prod_{p|a \vee p|b} p^{\text{máx}(v_p(a), v_p(b))}$$

vemos que satisface i) y ii).
En particular, si $a|m'$ y $b|m'$, $m \leq m'$.

Relación entre el mcd y el mcm

Veamos finalmente que: $[a,b]\cdot(a:b)=a\cdot b$ Como

$$(a:b)=\mathrm{mcd}(a,b)=\prod_{p|a\wedge p|b} p^{\mathrm{mín}(v_p(a),v_p(b))}$$

$$[a:b]=\mathrm{mcm}(a,b)=\prod_{p|a\vee p|b} p^{\mathrm{máx}(v_p(a),v_p(b))}$$

basta observar que:

$$\mathrm{máx}(m,n)+\mathrm{mín}(m,n)=m+n\ \forall\ m,n\in\mathbb{N}_0$$

para concluir que:

$$(a:b)\cdot[a:b]=\prod_p p^{\mathrm{mín}(v_p(a),v_p(b))+\mathrm{máx}(v_p(a),v_p(b))}$$

$$=\prod_p p^{v_p(a)+v_p(b)}=\left(\prod_p p^{v_p(a)}\right)\left(\prod_p p^{v_p(b)}\right)=a\cdot b$$

Parte IV

Otras aplicaciones

Cantidad de divisores

Teorema

Si

$$n = \prod_{p|n} p^{v_p(n)}$$

es la factorización estándar de n, entonces $d(n)$ = *cantidad de divisores positivos de n, puede calcularse como*

$$d(n) = \prod_{p|n} (v_p(n) + 1)$$

Ejemplo:

$$360 = 2^3 \cdot 3^2 \cdot 5^1 \Rightarrow d(360) = (3+1) \cdot (2+1) \cdot (1+1) = 4 \cdot 3 \cdot 2 = 24$$

De hecho, los divisores de 360 son

$$[1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360]$$

Demostración

Sea $D(n)$ el conjunto de divisores positivos de n. Por lo anterior

$$D(n) = \left\{ d : d = \prod_{p|n} p^{e(p)}, \forall p : 0 \leq e(p) \leq v_p(n) \right\}$$

Entonces la aplicación

$$d \mapsto (e_p(n))$$

define una biyección entre $D(n)$ y el producto cartesiano

$$\prod_{p|n} I_{v_p(n)}$$

donde

$$I_k = \{0, 1, 2, \ldots, k\}$$

Como $\#(I_{v_p(n)}) = v_p(n) + 1$ obtenemos el resultado.

Un ejercicio: Irracionalidad de las raices cuadradas

Vimos antes que $\sqrt{2} \notin \mathbb{Q}$. Usando el teorema fundamental de la aritmética podemos generalizar este hecho:

Enunciado

Si $n \in \mathbb{N}, n > 1$ no es el cuadrado de un entero, entonces $\sqrt{n} \notin \mathbb{Q}$.

Solución del ejercicio (1)

Observación

n es el cuadrado de un entero $\Leftrightarrow$ $v_p(n)$ es par para todo primo p.

$\Rightarrow$) si $n = m^2$ entonces $v_p(n) = 2v_p(m)$ luego $v_p(n)$ es par.
$\Leftarrow$) si $v_p(n)$ es par para todo primo p consideramos

$$m = \prod_{p|n} p^{v_p(n)/2}$$

Entonces m es entero (porque todos los exponentes lo son) y $m^2 = n$.

Solución del ejercicio(2)

Razonando por el absurdo, si $\sqrt{n} = \frac{a}{b}$ con $a, b \in \mathbb{N}$ y $b \neq 0$, tendríamos

$$n \cdot b^2 = a^2$$

Entonces para todo primo p

$$v_p(n) + 2\ v_p(b) = 2\ v_p(a) \Rightarrow v_p(n) = 2[v_p(a) - v_p(b)]$$

Se deduce que $v_p(n)$ es par para cada primo p, con lo cuál n sería el cuadrado de un entero. ¡absurdo! (pues contradice la hipótesis).
El absurdo provino de suponer que $\sqrt{n}$ es racional. Luego debe ser irracional.

Una generalización, para pensar

El siguiente enunciado generaliza el ejercicio anterior y también al ejercicio 28 de la práctica 4.

Enunciado

Sean $n, k \in \mathbb{N}, n, k > 1$. Si n no es la potencia k-ésima de un entero entonces $\sqrt[k]{n} \notin \mathbb{Q}$.