Apuntes de clases de Teoría de números

Grupo Estudiantil de Matemática

Actualizado a la fecha 14 de enero del 2018

Prefacio

Estos son los apuntes de clases de Teoría de números organizado por el Grupo Estudiantil de Matemática durante los meses de enero y febrero del año 2018.

Muchas gracias al Instituto de Matemática y Ciencias Afines por brindarnos sus ambientes para llevar a cabo las clases.

Por favor, cualquier sugerencia o aviso de error escribir a gem@uni.edu.pe o caznaranl@uni.pe.

Carlos Aznarán

Und. Jimmy Espinoza Palacios
Miembro del GEM
Facultad de Ciencias

Und. Bruno Goicochea Vilela
Presidente del GEM
Facultad de Ciencias

Tabla de contenido

Capítulo 1

Introducción

I. *Principio de inducción matemática*

Sea $\mathcal{P}$ un conjunto de números naturales tal que

a) $1 \in \mathcal{P}$.

b) Si $n \in \mathcal{P} \implies n + 1 \in \mathcal{P}$.

$\therefore \boxed{\mathcal{P} = \mathbb{N}}$.

II. *Principio del buen orden*

Si $\mathcal{A}$ es un conjunto no vacío de $\mathbb{N}$, entonces $\mathcal{A}$ *posee un elemento mínimo*.

1.1. Divisibilidad

Definición 1.1. *Sean d y n dos números enteros, se denotará*

$$\boxed{d \textit{ divide a } n \iff \textit{existe } c \in \mathbb{Z} \textit{ tal que } n = c \cdot n}$$

como $a \mid n$.
Si d no divide a n, es decir, si $\forall c \in \mathbb{Z}\colon n \neq c \cdot d$, se denotará como $d \nmid n$.

Propiedades de la operación $|$

1) $n \mid n$ para cualquier $n \in \mathbb{N}$ (Reflexividad).

2) Si $d \mid n$ y $n \mid m$, entonces $d \mid m$. (Transitividad).

3) Si $d \mid n$ y $d \mid m$, entonces $d \mid an + bm \; \forall a, b \in \mathbb{Z}$.

4) Si $d \mid n$, entonces $ad \mid an$.

5) Si $ad \mid an$ con $a \neq 0$, entonces $d \mid n$.

6) $1 \mid n$ para cualquier $n \in \mathbb{N}$.

7) $n \mid 0$ para cualquier $n \in \mathbb{N}$.

8) Si $0 \mid n$, entonces $n = 0$.

9) Si $d \mid n$ y $n \neq 0$, entonces $|d| \leqslant |n|$.

10) Si $d \mid n$ y $n \mid d$, entonces $|d| = |n|$.

11) Si $d \mid n$ con $d \neq 0$, entonces $\left(\frac{n}{d}\right) \mid n$.

1.2. Máximo común divisor

Definición 1.2. *Sean a, b y d números enteros. Si $d \mid a$ y $d \mid b$, entonces d es un divisor común de a y b.*

Teorema 1.1. *Dados los números enteros a y b, existe un divisor común d de a y b de la forma $d = ax + by$ para cualesquiera $x, y \in \mathbb{Z}$.*

Prueba: Por inducción matemática en $K = |a| + |b|$.

Si $K = 0$, entonces $a = b = 0$, esto es, $d = 0 \cdot a + 0 \cdot b$. ✓

Supongamos que se cumple para $K = 0, 1, \ldots, n-1$. (Hipótesis de inducción matemática).

Demostraremos para $\boxed{K = n = |a| + |b|}$.

Sin pérdida de generalidad, suponga que $|a| \geqslant |b|$. Así, si $|b| = 0$, entonces $b = 0$ y $|a| = n \implies d = n = (1)(\pm 1) + 0 \cdot b$.

Si $|b| \geqslant 1$, entonces para los números $|a|-|b|$ y $|b|$ se cumple la hipótesis:

$$\underbrace{|a|-|b|}_{\geqslant 0}+|b| = |a|-\cancel{|b|}+\cancel{|b|} = |a| < |a|+|b| = n.$$

Existe $d \in \mathbb{Z}$, $d \mid |a|-|b|$ y $d \mid |b|$. Además:

$$\begin{aligned}
d &= (|a|-|b|)\,x' + |b|y' \qquad\qquad \forall x', y' \in \mathbb{Z}\\
d &= |a|\underbrace{x'}_{x''} + |b|\underbrace{y'}_{y''}\\
d &= \underbrace{|a|}_{a,-a}x'' + \underbrace{|b|}_{b,-b}y''\\
d &= a\underbrace{x''}_{\pm x'} + b\underbrace{y''}_{\pm y'}
\end{aligned}$$

Pero $d \mid |a|$ y $d \mid |b|$, así $d \mid |a|-|b|$.
$\therefore$ Esto cumple la condición. $\blacksquare$

Teorema 1.2. *Sean a y b números enteros, existe solo un número $d \in \mathbb{Z}$ tal que*

1) $d \geqslant 0$.

2) $d \mid a$ *y* $d \mid b$.

3) *Si $e \mid a$ y $e \mid b$, entonces $e \mid d$ para cualquier $e \in \mathbb{Z}$.*

Prueba: Por la definición 1.2 y por el teorema 1.1, existe un d con las siguientes propiedades:

$$d \mid a \qquad\qquad d \mid b \qquad\qquad d = ax + by$$

Es claro que $-d$ también cumple esto. Elegimos $|d| = ax' + by'$ que cumpla 1) y 2).
Si $e \mid a$ y $e \mid b$, entonces de la propiedad 3) $e \mid ax' + by' = |d|$.
Así, $e \mid |d|$, en consecuencia $e \mid d$ y $|d|$ satisface 3).
Si existiese un d' que cumpla 1), 2) y 3), entonces de la afirmación 3):

$$d \mid a \text{ y } d \mid b \implies d \mid d'. \tag{1.1}$$

De forma similar:

$$d' \mid a \text{ y } d' \mid b \implies d' \mid d. \tag{1.2}$$

Pero de (1.1) y (1.2) junto con la propiedad 10) se obtiene que $\boxed{d = d'}$.

■

Definición 1.3. *Este número d es llamado máximo común divisor de a y b y se denota como $\operatorname{mcd}(a, b)$ o (a, b).*

Observación 1.1. *Si el $\operatorname{mcd}(a, b) = 1$, entonces a y b son llamados coprimos, primos entre sí (PESI) o primos relativos.*

Algunas propiedades del máximo común divisor

1) $(a, b) = (b, a)$.

2) $(a, (b, c)) = ((a, b), c)$.

3) $(ac, bc) = |c|(a, b)$.

4) $(a, 1) = (1, a) = 1$.

5) $(a, 0) = (0, a) = |a|$.

Teorema 1.3. *Si $a \mid bc$ y si $(a, b) = 1$, entonces $a \mid c$.*

Demostración. Como $(a, b) = 1$, entonces existen $\tilde{x}, \tilde{y} \in \mathbb{Z}$ de modo que

$$1 = a\tilde{x} + b\tilde{y} \tag{1.3}$$

Pero si multiplicamos (1.3) por c resulta

$$c = a(c\tilde{x}) + b(c\tilde{y}) \tag{1.4}$$

Así, $a \mid cx$ y $a \mid cy$ (explicar).

■

1.3. Números primos

Definición 1.4. *El número $n \in \mathbb{N}$ es llamado número primo si sus divisores positivos son 1 y n. Cuando n no es primo, será llamado número compuesto.*

Teorema 1.4. *Cada natural $n > 1$ o es primo o producto de números primos.*

Prueba: Por inducción sobre n.
Para $n = 2$ ✓
Supongamos que se cumple para $n = 2, 3, \ldots, k - 1$.
Demostraremos para $n = k$.

***)** Si k es un número primo.

***)** Si k no es un número primo, entonces k tiene por lo menos un divisor $d > 1$, por lo que $k = d \cdot c$ con $1 < c < k$ y $1 < d < k$.

Se cumple la hipótesis para c y d, entonces c y d son primos o productos de primos.

$$c = p_1 p_2 \cdots p_k \qquad (p_i : \text{primo}, k \geqslant 1).$$
$$d = q_1 q_2 \cdots q_m \qquad (q_i : \text{primo}, m \geqslant 1).$$

Así, $n = c \cdot d = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_m$ (se cumple la inducción). ■

Teorema 1.5. *Existen infinitos números primos.*

Prueba: Supongamos que $\boxed{\mathbb{P} = p_1 p_2 \cdots p_k}$ es el conjunto de todos los números primos que existen. Definimos:

$$N = p_1 p_2 \cdots p_k + 1$$

¿Qué tipo de número es N, es un primo o uno compuesto?
Claro está que N es mayor que $p_i, \forall i = 1, \cdots k$.
$N = p_1 p_2 \cdots p_k + 1 = q_1 q_2 \cdots q_t$.

$$\begin{array}{l} q_i \mid p_1 p_2 \cdots p_k + 1 \\ q_i \mid p_1 p_2 \cdots p_k \qquad\qquad (-) \\ \hline q_i \mid 1 \quad (\Longrightarrow \ \Longleftarrow) \end{array}$$

$\therefore$ Existen infinitos números primos. ■

Teorema 1.6. *Si p es un número primo y $p \nmid a$, entonces $(p, a) = 1$.*

Demostración. Sea d el máximo común divisor de p y a (ya que el teorema 1.1 nos asegura su existencia), $d = (p, a)$, entonces

$$d \mid p \quad \text{y} \quad d \mid a.$$

■

Teorema 1.7. *Sea p un número primo. Si $p \mid ab$, entonces $p \mid a$ o $p \mid b$.*

Demostración: Supongamos que $p \nmid a$ ($p \mid a$ ✓), entonces $(p, a) = 1$, en consecuencia, $p \mid ab$.

$$\boxed{a \mid bc \quad \text{y} \quad (a, b) = 1 \implies a \mid c.}$$

$\therefore p \mid b$. ■

Teorema 1.8. *Cada entero $n > 1$ se representa de forma única como producto de primos no necesariamente distintos, sin importar el orden.*

Prueba: Por inducción en n. Cuando $n = 2$ (se cumple: 2,3,…,n-1.) $n = p_1 p_2 \cdots, p_s = q_1 q_2 \cdots q_t$ $(s = t)$. $(s, t \geqslant 1)$
$p_1 \mid q_1 q_2 \cdots q_t \implies p_1 \mid q_1 \implies p_1 = q_1$. ■

Observación 1.2. *Si se desea representar a n como producto de primos distintos (donde cabe la posibilidad en que se repitan algún número primo), podemos escribir:*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = \prod_{i=1}^{k} p_i^{a_i}$$

Teorema 1.9. *Si $n = \prod_{i=1}^{r} p_i^{a_i}$, entonces un divisor de n tiene la forma*

$$\prod_{i=1}^{r} = p_i^{c_i}, \quad 0 \leqslant c_i \leqslant a_i.$$

Observación 1.3. *Sea la sucesión de números primos*

$$p_1 = 2, p_2 = 3, p_3 = 5, \ldots,$$

entonces $n = \prod_{i=1}^{\infty} p_i^{a_i}$, $a_i \geqslant 0$.

Teorema 1.10. *Sean $a = \prod_{i=1}^{\infty} p_i^{a_i}$ y $b = \prod_{i=1}^{\infty} p_i^{b_i}$, entonces el máximo común divisor de a y b es*

$$(a, b) = \prod_{i=1}^{\infty} p_i^{c_i} \geqslant 0, \text{ donde } c_i = \min\{a_i, b_i\} \leqslant a_i, b_i.$$

Demostración: ***)** $\prod_{i=1}^{\infty} p_i^{c_i} \mid a \quad \wedge \quad \prod_{i=1}^{\infty} p_i^{c_i} \mid b.$

*) $e \mid a \quad \wedge \quad e \mid b, e = \prod_{i=1}^{\infty} p_i^{e_i}$.

Pero, $e_i \leqslant a_i$ y $e_i \leqslant b_i$,

$$\implies e_i \leqslant \min\{a_i, b_i\} = c_i.$$

$$e = \prod_{i=1}^{\infty} p_i^{e_i} \mid \prod_{i=1}^{\infty} p_i^{c_i} = (a,b).$$

■

Teorema 1.11. *Sean a y b números enteros con $b > 0$, entonces existen únicos $q, r \in \mathbb{Z}$ tal que:*

$$a = bq + r, \quad 0 \leqslant r < b.$$

Además, $r = 0 \iff b \mid a$.

Demostración: Fijando $\underline{b}$ y por inducción en $a \in \mathbb{N}$. Si $a = 0$, entonces $a = b \cdot 0 + 0$. ✓
Supongamos que se cumple para $a = 0, 1, \ldots, k-1$.
Para $a = k$. $k - 1 = b \cdot q' + r', 0 \leqslant r' < b$.

$$\longrightarrow k = bq' + (r'+1). \quad 1 \leqslant r' + 1 < b + 1.$$

- •) Si $1 \leqslant r' + 1 < b$ ✓
- •) Si $r' + 1 = b \rightarrow r' = b - 1 \implies$

■

Capítulo 2

Ejercicios

2.1. Lista N$^\circ 1$

1. Un número racional a/b con $(a,b)=1$ se llama *fracción reducida*. Si la suma de dos fracciones reducidas es un entero, es decir, si $(a/b)+(c/d)=n$. Demostrar que entonces $|b|=|d|$.

2. Si $(a,b)=1$, entonces $(a+b,a-b)$ o es 1 o es 2.

3. Si $(a,b)=1$, entonces $(a+b,a^2-ab+b^2)$ o es 1 o es 3.

4. Si $(a,b)=1$, entonces $(a^n,b^k)=1$ para todo $n\geqslant 1, k\geqslant 1$.

5. Un entero se llama *sin cuadrados* si no es divisible por el cuadrado de ningún primo. Probar que, para cada $n\geqslant 1$, existen $a>0$ y $b>0$, unívocamente determinados, tales que $n=a^2b$, en donde b es sin cuadrados.

6. Probar que $\dfrac{21n+4}{14n+3}$ es irreducible para todo número natural n.

7. Sean $\{a,b,x,y\}\subset\mathbb{N}$. Si $(a,b)=1$ y $ab=c^n$, probar que $a=x^n$ y $b=y^n$ para algunos x,y enteros positivos.

8. Hallar $\left(a^{2^m}+1,a^{2^n}+1\right)$ en función de a.

9. Sean $\{a, b, x, y\} \subset \mathbb{N}$. Si $(a, b) = 1$ y $x^a = y^b$ entonces probar que $x = n^b$ e $y = n^a$ para algún entero positivo.

10. Si $\{a, m, n\} \subset \mathbb{N}$ con $a > 1$, probar que $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

11. Sea n un entero positivo y sea S un conjunto de enteros positivos menores o iguales a $2n$ tal que si a y b están en S y a y b son diferentes, entonces a no divide a b. Hallar el máximo número de elementos de S.

12. Hallar todos los pares de enteros positivos (a, b) tales que $a \mid b + 1$ y $b \mid a + 1$.

13. Hallar todos los pares de enteros positivos (a, b) tales que $a \mid 8b+1$ y $b \mid 8a + 1$.

14. Halle todos los números enteros positivos n tales que el conjunto $\{n, n + 1, n + 2, n + 3, n + 4, n + 5\}$ puede ser particionado en dos subconjuntos de modo que el producto de los números en cada subconjunto sea igual.

15. Sea m y n números enteros tales que:

$$\frac{m}{n} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319}$$

Probar que m es divisible por 1979. Ayuda: 1979 es un número primo.

Mis notas de estudio

Divisibilidad

Definición 2.1. *Un entero b es divisible por un entero a, no cero, si existe un entero x tal que $b = ax$ y se escribe a $a \mid b$. En el caso en que b no sea divisible por a se escribe $a \nmid b$.*

Teorema 2.1. *Sean $\{a, b, c, x, y\} \subset \mathbb{Z}$, las siguientes proposiciones son verdaderas:*

1) *Si $a \mid b$, entonces $a \mid bc$ para cualquier entero c.*

Prueba:

De la definición (2.1) se sigue que existe algún entero m tal que $b = a \cdot m$. Ahora, sea $c \in \mathbb{Z}$ fijo y arbitrario. Así, el número $bc = a \cdot m(c)$ y de (2.1) existe un entero $d = m(c)$ tal que $b = a \cdot d$, por lo tanto $a \mid bc$. ■

1) *Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*

Prueba:

De la definición (2.1) se sigue que existen los entero m_1 y m_2 tales que $b = a \cdot m_1$ y $c = b \cdot m_2$. Pero c es igual a $b \cdot m_2 = (a \cdot m_1) \cdot m_2 = a \cdot (m_1 \cdot m_2)$, es decir, existe un entero $m_3 = m_1 \cdot m_2$ tal que $c = a \cdot m_3$, por lo tanto, de (2.1) $a \mid c$. ■

1) *Si* $a \mid (b_1, b_2, \ldots, b_n)$ *para algún* $n \in \mathbb{N}$*, entonces* $a \mid \sum_{j=1}^{n} b_j x_j$ *para cualesquiera* x_j.

Prueba:

De la definición (2.1) se sigue que existen n números $m_1, m_2, \ldots, m_n$ tales que $b_j = a \cdot m_j$ cuando $j \in \{1, 2, \ldots, n\}$. $\blacksquare$

1) *Si* $a \mid b$ *y* $b \mid a$*, entonces* $a = \pm b$*.*

Prueba:

$\blacksquare$