Proyecto Compilando Conocimiento

Matemáticas Discretas

Teoría de Números

Una Pequeña Introducción

Autor:
Rosas Hernandez Oscar Andres

Índice general

Capítulo 1

Enteros y Naturales

1.1. Principio de Buen Orden

Definición Formal

1.2. Divisibilidad

Definición Formal

Dados dos números cualquiera $a, b \in \mathbb{Z}$. Decimos que la proposición **"b" divide a "a"** $b|a$ es verdad si y solo si $\exists q \in \mathbb{Z},\ a = bq$.

Definición Alterna

Veamos que lo que de verdad nos estan preguntando si es que $\frac{a}{b} \in \mathbb{Z}$.

Ya que de ser así eso quiere decir que podemos escribir a a como $a = bq$. Y con esto logramos ver que $\frac{bq}{b} = q$ y habiamos dicho que $q \in \mathbb{Z}$.

Por lo tanto podemos resumir esto en que: "a divide a b si y solo si es que $\frac{a}{b}$ continua estando en los enteros"

$$b|a \ \Leftrightarrow \ \frac{a}{b} \in \mathbb{Z}$$

Ideas Imporantes

- Si $b|a$ y $b \neq 0$ entonces q es único.
- Si $b|a$ y $a \neq 0$ entonces $|b| \leq |a|$.

  Demostración:

  Supongamos entonces que b divide a a y que $a \neq 0$, por lo tanto la frase $a = bq$ nos da mucha información, pues obliga a que b y q no sean ninguno 0, entonces tenemos que $a = bq$ donde $b \neq 0$ y $q \neq 0$.

  Luego ya que no son 0, tenemos que $|q| \geq 1$ y $|b| \geq 1$, ya que sabemos como funcionan los números enteros tenemos que sin importar cuanto valgan q y b se cumple que $|b||q| \geq |b|$ esto es lo mismo que $|bq| \geq |b|$ y sabemos que $a = bq$, por lo tanto tenemos que $|a| \geq |b|$.

  Esto es lo mismo que $|b| \leq |a|$

Propiedades de Divisilibidad

- $b|b$

  Demostración:

  Basta con ver que si $a = b$ entonces $b = bq$, por lo tanto $q = 1$. Y listo, $1 \in \mathbb{Z}$.

- $b|0$

  Demostración:

  Basta con ver que si $a = 0$ entonces $0 = bq$, por lo tanto $q = 0$. Y listo, $0 \in \mathbb{Z}$.

- $1|a$ y también $-1|a$

  Demostración:

  Basta con ver que si $b = \pm 1$ entonces $a = \pm q$, por lo tanto $q = \pm a$. Y listo, $\pm a \in \mathbb{Z}$.

- $0|a$ si y solo $a = 0$

  Demostración:

  Basta con ver que tenemos $a = 0q$, esto es lo mismo que $a = 0$.

- $b|1$ si y solo si $b = 1$ ó $b = -1$

  Demostración:

  Sabemos que $a = 1 = bq$, esto nos obliga a que $b = \frac{1}{q}$, ahora tenemos que recordar que $b, q \in \mathbb{Z}$, por lo tanto $q = 1$ o bien $q = -1$ que es lo mismo que decir que $b = 1$ ó $b = -1$.

- $b|a$ y $a|b$ si y solo si $a = \pm b$

  Demostración:

  Sabemos que $a = bq_1$, y $b = aq_2$ por lo tanto podemos sustituir, $a = (aq_2)q_1$ por lo tanto $1 = (q_1)(q_2)$, que es lo mismo que $\frac{1}{q_2} = q_1$ ahora que para q_1 siga en los $\mathbb{Z}$, $q_2 = \pm 1$ por lo tanto $q_1 = \pm\frac{1}{1} = \pm 1$ por lo tanto tenemos que $a = bq_1$ que es lo mismo que decir que $a = \pm b$.

- Si $b|a$ y $a|c$ entonces $b|c$

  Demostración:

  Sabemos que $a = bq_1$, y $c = aq_2$ por lo tanto podemos sustituir, $c = (bq_1)q_2$ que es lo mismo que $c = bq_3$, donde $q_3 = q_1q_2$ donde $q_3 \in \mathbb{Z}$. Y ya que $c = bq_3$ podemos decir que $b|c$.

- Si $b|a$ y $b|c$ entonces $b|a+c$ y $b|a-c$

  Demostración:

  Sabemos que $a = bq_1$, y $c = bq_2$ por lo tanto podemos decir que sumar o restar ambas ecuaciones, lo que nos daría $a \pm c = bq_1 \pm bq_2$ que es lo mismo que $a \pm c = b(q_1 \pm q_2)$ por lo que podemos decir que $b|a \pm c$.

- Si $b|a$ entonces $b|ak$ $\forall k \in \mathbb{Z}$.

  Demostración:

  Sabemos que $a = bq$ por lo mismo podemos decir que $ak = b(qk)$ por lo tanto $b|ak$.

- $b|a$ si y solo si $b|-a$ si y solo si $-b|a$ si y solo si $-b|-a$

  Demostración:

  Sabemos que existe q_1 tal que $a = bq_1$ para nuestro primer ssi basta con decir que $-a = b(-q_1) = bq_2$ y listo, encontre a q_2 con lo que puedo afirmar que $b|-a$.

  Para el segundo basta con ver que $a = -bq_3$ donde $q_3 = q_2$, con lo que puedo afirmar que $-b|a$.

  Para el último ssi basta con con ver que $-a = -bq_4$ donde $q_4 = q_1$ así que puedo afirmar que $-b|-a$.

1.3. Algoritmo de División

Definición Formal

Dados dos enteros a, b donde $b \neq 0$, existen otros dos enteros únicos q, r, donde $0 \leq r < |b|$ tal que se cumple:

$$a = bq + r \tag{1.1}$$

Vemos que basicamente nos dice cuántas veces cabe b en a sin pasarse (esto es q) y cuantos le faltan para alcanzar a a (esto es r).

Demostración:

El primer paso es crear el conjunto $Residuos = \{a - |b|q \ \mid \ q \in \mathbb{Z}, (a - |b|q) \geq 0\}$.

Ahora lo primero que tenemos que ver que es $|Residuos| \neq 0$. Para hacerlo veamos un contraejemplo, es decir $a < |b|$, entonces intenta a $q = -1$ y vemos que $a + |b|$ siempre sera mayor o igual que 0. Si $a > |b|$, entonces intenta a $q = 1$ y vemos que $a - |b|$ siempre sera mayor o igual que 0. Finalmente si $a = |b|$ cualquiera de los 2 ejemplos anteriores te sirven. Por lo tanto mínimo *Residuos* tiene mínimo un elemento.

Esto es un conjunto que basicamente contiene a los residuos, o visto de otra manera a los números que salen como resultado de sumarle multiplos de $|b|$ a a y que son mayores que 0.

Ahora gracias al principio de buen orden (y que *Residuos* es el conjunto de los Naturales más el cero) podemos llamar a r al elemento mas pequeño de este conjunto.

Ahora, gracias a la definición del conjunto *Residuos* podemos decir que $r = a - |b|q_1$ que es decir $a = |b|q_1 + r$.

Ahora podemos poner esto como $a = bq + r$ donde si $b < 0 \ \Rightarrow \ q = -q_1$ y si $b > 0 \ \Rightarrow \ q = q_1$.

Para ver que $0 \leq r < |b|$, bueno, es mayor o igual que 0 porque pertenece a los Naturales más el cero, ahora para ver que es menor que $|b|$, basta con ver que si no fuera así pasaría que $r - |b| \geq 0$ (donde r es el elemento más pequeño del conjunto *Residuos*) que es lo mismo que poner $(a - |b|q_1) - |b| \geq 0$ que es lo mismo que $a - |b|(q_1 + 1) \geq 0$, ahora basta con ver que esa no es la r más pequeña, pues entonces si $a - |b|(q_1 + 1) \geq 0$, también $a - |b|q_1 \geq 0$, por lo que la nueva r_2 (donde $r_2 = a - |b|q_1$), es mas pequeña que r, pero elegimos a r como la más pequeña, por lo tanto contradicción.

Y ya por fin, para demostrar que q, r son únicos dados a, b, tendría que pasar que $a = bq_1 + r_1 = bq_2 + r_2$.

Recordemos que r debe de ser única, pues r es el menor elemento del conjunto del que tendríamos que sacar a la otra, así que r solo hay una.

Dado eso, tenemos que $a = bq_1 + r = bq_2 + r$ que es lo mismo que $bq_1 = bq_2$ que es lo mismo que $q_1 = q_2$ y bingo. Demostrado.

1.3.1. Par e Inpar

Dado un 2 como divisor, osea $b = 2$, nuestra r siempre será 0 ó 1. Digo recuerda que $0 \leq r < |b|$.

Pares

Por lo tanto puedo definir a un número entero par como aquellos números que podemos escribirlos gracias al algoritmo de la división como $2q+0$ o de manera más común como $2k$.

$$\begin{aligned} Pares &= \{a \in \mathbb{Z} \mid a = 2q + 0,\ q \in \mathbb{Z}\} \\ Pares &= \{2k \mid k \in \mathbb{Z}\} \end{aligned} \tag{1.2}$$

Inpares

Por lo tanto puedo definir a un número entero inpar como aquellos números que podemos escribirlos gracias al algoritmo de la división como $2q+1$ o de manera más común como $2k+1$.

$$\begin{aligned} Pares &= \{a \in \mathbb{Z} \mid a = 2q + 1,\ q \in \mathbb{Z}\} \\ Pares &= \{2k + 1 \mid k \in \mathbb{Z}\} \end{aligned} \tag{1.3}$$

Y de esto sacamos algunas ideas bastante obvias:

Ideas Importantes

- Un número n es un cuadrado $n = m^2$ si y solo si al aplicarle el algoritmo de la división con $b = 4$ implica que $r = 1$ ó $r = 0$.

  Demostración:

  Si es un número par $m = 2k$, entonces $(2k)^2$ que es igual a $4k^2$ donde podemos decir que $n = 4(k^2) + 0$.

  Si es inpar $m = 2k + 1$, entonces $(2k + 1)^2$ que es igual a $4k^2 + 4k + 1$ donde podemos decir que $n = 4(k^2 + k) + 1$.

Capítulo 2

Combinatoria

2.1. Definición

Una relación R entre dos conjuntos A y B es ante todo otro conjunto, una relación binaria es aquella que es en el fondo un conjunto de pares ordenados (x,y) donde x es un elemento de A, y así mismo y es un elemento de B.

Este nuevo conjunto R nos muestra como es que esta relacionados algunos (o todos) elementos de A con otros elementos de B.

Definiciones Formales

Una Relación $R : A \to B$ es un subconjunto de $A \times B$.

Solemos escribir la proposición $(x, y) \in R$ como xRy para que se vea más bonito.

Solemos escribir la proposición $(x, y) \notin R$ como $x \not R\, y$ para que se vea más bonito.