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. 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 por casos, si $a < |b|$, 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.

1.2.1. 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 $n = 4(k^2 + k) + 1$.

1.3. 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 $\exists q \in \mathbb{Z},\ a = bq$.

- Los divisores de a son el conjunto:

$$Divisores = \{x \in \mathbb{Z} \mid x|a\}$$

- Los múltiplos de b son:

$$Multiplos = \{x \in \mathbb{Z} \mid b|x\}$$

Definición Alterna

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

Podemos entonces enunciar que: "a divide a b si y solo si es que $\frac{a}{b}$ continua estando en los enteros".

Demostración:

Podemos ver que nos estan preguntando lo mismo, ya que si mi definición alterna es verdad, 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 $q \in \mathbb{Z}$.

1.3.1. Ejemplos

Supongamos que elegimos la proposición $5|35$.

Entonces lo que nos estan preguntando en el fondo es si $\frac{35}{5} \in \mathbb{Z}$ podemos ver que si, pues $\frac{35}{5} = 7$.

Podemos también decir que:

- Los divisores de 35 son:

$$Divisores = \{b \in \mathbb{Z} \mid b|35\}$$
$$Divisores = \{\pm 1, \pm 3, \pm 7, \pm 35\}$$

- Los múltiplos de 5 son:

$$Multiplos = \{a \in \mathbb{Z} \mid 5|a\}$$
$$Multiplos = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$

1.3.2. 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 $b|a \pm c$

  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 $-b| - a$.

- 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 $|b| \leq |a|$

1.4. Máximo Común Divisor: GCD/MCD

Definición Formal

Dados dos números cualquiera $a, b \in \mathbb{Z}$ pero con mínimo alguno de ellos dos diferentes de 0.

Entonces decimos que el máximo común divisor de a y b denotado por $MCD(a, b) = GCD(a, b)$ es el entero positivo d que satisface:

- $d|a$ y $d|b$
- Si $c|a$ y $c|b$ entonces $c \leq d$.

Ideas:

Decimos que d es un división común de a y b si $(d|a) \wedge (d|b)$.

Ahora podemos construir el conjunto de los divisores comúnes. $Divisores = \{d \in \mathbb{Z} \mid (d|a) \wedge (d|b)\}$

Ahora si, con todo esto listo, podemos ver que este conjunto nunca estará vació. como 1 es un divisón común de todos los enteros.

Ahora podemos ver que el conjunto no es infinito siempre que alguno de ellos no sea cero, hay sólo una cantidad finita de divisores comunes positivos. Dentro de ellos hay uno que es el mayor.

La segunda condición se asegura de que d sea el máximo elemento dentro del conjunto.

1.4.1. Propiedades de MCD/GCD

Antes que nada, recuerda que para que tenga sentido hablar del máximo común divisor alguno de los dos a, b debe de ser diferente de cero. Porfis.

Recuerda también llamaré c a lo que salga de $c = max(|a|, |b|)$.

Ahora supongamos que es a el que es diferente de 0, después de todo $MCD(a, b) = MCD(b, a)$

- Siempre se cumple que $0 < MCD(a, b) \leq max(|a|, |b|)$

  Demostración:

  Para lo primero basta con recordar que 1 divide a todos los enteros, así que 1 siempre será un divisor común, por lo tanto, cualquier otro divisor que aspire a ser el MCD/GCD tendría que que ser mayor que 1, o bien, si son primos relativos, ser el 1.

  Basta con pensar que $c = max(|a|, |b|)$ es más grande o igual que 1, y ahora veamos que es imposible que existe un número n que sea el máximo común divisor donde $c < n$. Ya que de ser así pasa que $max(|a|, |b|) < n$. Digamos que puedo escribir a $n = c + k$.

  Y eso nos díria que si $|(c + k)|a$ y $a \neq 0$ entonces $|c + k| \leq |a|$

  Pero, c es positiva, y también k, por lo tanto la proposicíon $|c + k| \leq |a|$ es falsa. Espero que se vea claro porque, ya si c es el mayor de sus valores absolutos, si le añadimos otro natural a ese número solo se puede hacer más grande, haciendo imposible la frase $|c + k| \leq |a|$.

  Por lo tanto, es imposible que exista dicha n.

  Y el máximo común divisor queda atrapado en esos límites.

- Siempre se cumple que $MCD(a, 0) = GCD(a, 0) = |a|$

  Demostración: Basta con pensar que $|a|$ divide a ambos, y es más grande que 1, así que vamos bien, y despúes pensar que si existiríera algún divisor más grande que $|a|$ entonces se cumpliría que $|(|a| + k)|a$ por lo tanto tambíen se cumpliría lo que dijimos antes, (que si $|(|a| + k)|a$ y $a \neq 0$ entonces $|(|a| + k)| \leq |a|$) y eso claro es una contradicción por lo tanto, $|a|$ es siempre el mayor divisor común.

- Siempre se cumple que $GCD(a, b) = GCD(-a, b) = GCD(a, -b) = GCD(-a, -b)$

  Demostración: Si $d = GCD(a, b)$ entonces también se que si c es también un divisor común $c \leq d$, pero vemos que $d| - a$ y $d| - b$.

  Ahora, vemos que d es también un divisor común, y es que es el mayor, porque si $c| - a$ y $c| - b$ ya habiamos dicho que $c \leq d$.

  Literalmente no hay otra forma. Demostrado.

1.4.2. Identidad de Bezout

Existen unos $m, n \in \mathbb{Z}$ llamados coeficientes de Bezout tal que se cumple siempre que:

$$MCD(a, b) = GCD(a, b) = am + bn \tag{1.4}$$

Demostración:

Este "teorema" parece bastante importante, así que veamoslo con más detalle, nos dice que podemos escribir al MCD/GCD de a, b como una combinación lineal de ellos.

Ahora, concentremos en las combinaciones lineales que sean positivas, hagamos el conjunto $Combinaciones = \{am + bn \mid m, n \in \mathbb{Z},\ am + bn > 0\}$.

Con esto tenemos todas las combinaciones lineales positivas. También sabemos que no esta vacío ese conjunto, pues mínimo $max(|a|, |b|)$ esta ahí dentro.

Por el principio del buen orden, este conjunto tiene un primero elemento. Llamemos d a ese elemento, donde vemos que $0 < d \leq max(|a|, |b|)$, esto se parece a nuestro mínimo común múltiplo.

Veamos si es un divisor común primero, por el algoritmo de la división podemos decir que podemos escribir $a = dq + r$ y también como $d \in Combinaciones$, osea $d = am + bn$ podemos decir que $a = (am + bn)q$.

Por lo tanto veamos que pasa si despejo r:

$r = a - dq = a + d(-q) = a + (am + bn)(-q) = a(1 - qm) + b(-qn)$

Si no te has dado cuenta, esta de la forma $ax+by$, osea que r también debería estar en $Combinaciones$, pero creí que d era la combinación más pequeña, la única forma de que esto no sea una contradicción es que $r = 0$, pues $0 \leq r \leq (am + bn)$ (Inteligente, ¿no?).

Así podemos darnos cuenta de que si tomamos al menor elemento de la forma $am+bn$ este siempre tiene que dividir a a, y de hecho a no tiene nada de especial. Lo mismo pasa con b.

Ok, ahora sabemos que d es un divisor común, para ver que es el más pequeño simplemente imaginate otro, como x un divisor positivo común de a y b, existen entonces enteros s, t tales que $a = xs \wedge b = xt$ y como vimos podemos poner a d como $d = am + bn$.

Tenemos que $d = am + bn = (xs)m + (xt)n = x(sm + tn)$, si te das cuenta la proposición $x|d$ es cierta, pues $d = x(sm + tn)$, por lo que podemos decir que $|x| \leq |d|$, pero vamos, ambos son positivos, eso de antes es lo mismo que $x \leq d$, por lo tanto por definición d es nuestro máximo común divisor.

1.4.3. Propiedades de MCD/GCD: Bezout Edition

- Si tengo 3 números $a, b, c \in \mathbb{Z}$ donde c y alguno de los dos restantes a, b no son cero, entonces c se puede escribir como una combinación lineal de a y b si y solo si c es el GCD MCD de a, b o bien si es uno de sus múltiplos.

  Demostración: Vamos, literalmente acabo de demostrar que el GCD es equivalente a escribirlos como combinación lineal, ahora también funciona con los múltiplos, pues si d es el GCD y c un múltiplo, entonces tenemos que $d = am + bn$ y también $c = kd$.

  Por lo tanto nuestra ansiada combinación lineal es simplemente $c = a(km)+b(kn)$. Y ¡Bingo!

- El conjunto $Combinaciones = \{am + bn \mid m, n \in \mathbb{Z},\ am + bn > 0\}$. es precisamente el conjunto de múltiplos de GCD(a,b).

  Demostración: Sea $d = GCD(a, b)$, si $d|m$ entonces $m = dc$ para algún $c \in \mathbb{Z}$ y entonces $m = dc = c(am + bn) = a(cm) + b(cn)$.

  Así que cualquier multiplo de d estará en este conjunto.

  Además es claro que d divide a cualquier combinación lineal de a,b por ser un divisor común.

1.4.4. Primos Relativos

Decimos que dos enteros a y b son primos relativos si $mcd(a, b) = 1$.

Ideas Interesantes

- Dos enteros a, b son primos relativos sí y sólo si,existen enteros $x, y \in \mathbb{Z}$ tales que $1 = am + bn$.

  Demostración: Esto es literalmente un corolario de la Identidad de Bezout, porque si son primos relativos, entonces $GCD(a, b) = 1$, y por la identidad existen x, y tal que $1 = am+bn$.

- Sea $d = GCD(a, b)$ La pareja de $(\frac{a}{d}, bd)$ siempre son primos relativos.

  Demostración:

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.