Proyecto Compilando Conocimiento

Matemáticas Discretas

Teoría de Números

Una Pequeña Introducción

Autor:
Rosas Hernandez Oscar Andres

Índice general

Capítulo 1

Naturales

1.1. Principio de Buen Orden

Definición Formal

Capítulo 2

Divisibilidad

2.1. 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:

$$a = bq + r \tag{2.1}$$

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.

2.1.1. 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 $2k$.

$$\begin{aligned} Pares &= \{a \in \mathbb{Z} \mid a = 2q + 0,\ q \in \mathbb{Z}\} \\ Pares &= \{2k \mid k \in \mathbb{Z}\} \end{aligned} \tag{2.2}$$

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 $2k+1$.

$$\begin{aligned} Pares &= \{a \in \mathbb{Z} \mid a = 2q + 1,\ q \in \mathbb{Z}\} \\ Pares &= \{2k + 1 \mid k \in \mathbb{Z}\} \end{aligned} \tag{2.3}$$

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

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

- 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: "b divide a a 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 $q \in \mathbb{Z}$.

2.2.1. 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:

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

2.2.2. 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 $a|b$ y $a|b \pm c$ entonces $a|c$

  Demostración:

  Sabemos que $b = aq_1$, y $b \pm c = aq_2$, si restamos tenemos que $b \pm c - b = aq_2 - aq_1$, que es lo mismo que $\pm c = (q_2 - q_1)a$, que es lo mismo que $c = \pm(q_2 - q_1)a$ que es lo mismo que $c = q_3 a$.

- 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 $|b| \leq |a|$

2.3. 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.

2.3.1. 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.

- El $GCD(a,b) = GCD(a, b \pm ka)$ donde $k \in \mathbb{N}$

  Demostración:

  Vamos a hacer una primera aproximación diciendo que $GCD(a,b) = GCD(a, \pm b)$, ya si se demostrará que eso fuera cierto, creo que es obvio que puedes aplicar el proceso varias veces para llegar a $GCD(a,b) = GCD(a, \pm kb)$ donde $k \in \mathbb{N}$.

  Para hacerlo lo que vamos a demostrar es que ambos conjuntos de divisores, el primero el de a, b (llamemoslo $Divisores1$) y el de $a, b \pm a$ ($Divisores2$) es el mismo conjunto.

  Si $x \in Divisores1$ entonces sabemos que $x|a$ y $x|b$, entonces gracias a una propiedad de divisibilidad ya demostre antes (Si $b|a$ y $b|c$ entonces $b|a \pm c$) sabemos que $x|a \pm b$, es decir $x \in Divisores2$. Además, si $y \in Divisores2$ entonces $y|a$ y $y|a \pm b$, por lo tanto (sabiendo que Si $a|b$ y $a|b \pm c$ entonces $a|c$) $y|b$, por lo tanto $y \in Divisores1$. Por lo que vemos que son el mismo conjunto.

  Si son el mismo conjunto de divisores naturales, tendrán el mismo máximo elemento. ¡Bingo!

2.3.2. Identidad de Bezout

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

$$MCD(a,b) = GCD(a,b) = am + bn \tag{2.4}$$

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.

2.3.3. 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.

- La pareja de $m, n \in \mathbb{Z}$ llamados coeficientes de Bezout, ya sabes aquella que cumple que $GCD(a, b) = am + bn$, siempre serán coprimos.

  Demostración:

  Sabemos que existen enteros m, n tal que $d = am + bn$ por la identidad de Bezout, además como d es un divisor común podemos escribir $a = dq_1$ $b = dq_2$ para algunos enteros q_1, q_2.

  Por lo que $d = am + bn = dmq_1 + dnq_2 = d(mq_1 + nq_2)$, por lo tanto tenemos que $1 = mq_1 + nq_2$.

  Esto es muy importante, porque nos dice que los enteros m y n son primos relativos (Dos enteros a, b son primos relativos sí y sólo si,existen enteros $x, y \in \mathbb{Z}$ tales que $1 = am + bn$).

  Y bingo, ahí esta nuestra pareja de primos relativos.

- Supón $GCD(a, b) = 1$ y que $a|bc$, entonces $a|c$.

  Demostración:

  Esta idea suena muy específica, pero creeme que es muy útil.

  Además demostrarlo es más sencillo de lo que te imaginas, sabemos que por la identidad de Bezout $am + bn = 1$, ahora multiplica todo por c y tendremos que: $amc + bnc = c$.

  Además recuerda que $a|bc$, es decir $bc = aq$, por lo tanto podemos decir que $amc + aqc = c$ esto es lo mismo que $a(mc + qc) = c$ por lo tanto podemos decir que $q = mc + qc$ y tener que $c = aq$, es decir $a|c$.

2.3.4. Primos Relativos

Decimos que dos enteros a y b son primos relativos o coprimos 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 $(\frac{a}{d}, \frac{b}{d})$ siempre son primos relativos.

  Demostración:

  Sabemos que existen enteros m, n tal que $d = am + bn$ por la identidad de Bezout, además como d es un divisor común podemos escribir $a = dq_1$ $b = dq_2$ para algunos enteros q_1, q_2.

  Por lo que $d = am + bn = dmq_1 + dnq_2 = d(mq_1 + nq_2)$, por lo tanto tenemos que $1 = mq_1 + nq_2$.

  Esto es muy importante, porque nos dice que los enteros q_1 y q_2 son primos relativos (Dos enteros a, b son primos relativos sí y sólo si,existen enteros $x, y \in \mathbb{Z}$ tales que $1 = am + bn$).

  Por lo tanto basta con ver que $q_1 = \frac{a}{d}$ y que $q_1 = \frac{b}{d}$.

  Y bingo, ahí esta nuestra pareja de primos relativos.

2.4. Algorítmo de Euclides

Definición Formal

Un algoritmo eficiente para calcular el máximo común divisor de dos enteros se puede conseguir aplicando repetidamente el algoritmo de Euclides.

Si intentamos calcular $GCD(a, b)$ y sabemos del algoritmo de la división que $a = bq + r$ entonces podemos simplificar el problema ya que:

$$GCD(a, b) = GCD(b, r) = GCD(b, b\,\%a) \tag{2.5}$$

Podemos seguir aplicando esta identidad hasta que el $GCD(a, b)$ séa muy obvio.

Demostración:

Esta afirmación es la importante: $GCD(a, b) = GCD(b, r)$ donde r es el residuo del algoritmo de la división donde $a = bq + r$.

Para probarla lo que haremos sera darnos cuenta que el conjunto de divisores comunes de a y b será el mismo que el de b y r. Es decir para una d cualquiera que sea un divisor común de a y b si y solo si d es un divisor de b y de r.

Veamos que podemos probar esto gracias a que podemos verlo como una implicación de dos lados.

Por un lado si d es un divisor de a y b, es decir $d|a$ y $d|b$ sabemos que $d|a-k$, es un resultado que ya habiamos probado, pero que pasa si decimos que esa k no es otra bq, ya que de $a = bq + r$ podemos ver como $r = a - bq = a - k$, con lo que vemos que $d|r$, por lo tanto vimos que para cualquier d que divida a a, b también lo hará con b, r.

Por otro lado supón que d es un divisor común de b y r, entonces $d|b$ y $d|r$, por lo tanto $d|bq$ y si ya sabemos que $d|bq$ entonces también lo hace con $d|bq + r$, por lo tanto $d|a$, por lo tanto vimos que para cualquier d que divida a b, r también lo hará con a, b.

Y si tienen exactamente los mismos elementos en cada conjunto de divisores comunes entonces creo que es bastante obvio que el máximo elemento de cada conjunto será el mismo, es decir, tienen el mismo GCD.

2.4.1. Como Aplicarlo

Esto ya nos muestra una forma de calcular el máximo común divisor de dos números a, b de una manera más sencilla pues en principio b, r son números más pequeños.

- El primer paso es aplicar el algoritmo para la división:

  $$a = bq_1 + r_1 \quad 0 \leq r_1 < b$$

  Si da la casualidad de que $r_1 = 0$ entonces $b|a$, por lo que $GCD(a, b) = b$. Y listo, encontrado.

  Si no tuvimos tanta suerte podemos al menos saber que $GCD(a, b) = GCD(b, r_1)$, así que volvemos a aplicar el algoritmo de la división.

- Ahora tenemos que

  $$b = r_1q_2 + r_2 \quad 0 \leq r_2 < r_1$$

  Si da la casualidad de que $r_2 = 0$ entonces $r_1|b$, por lo que $GCD(a, b) = GCD(b, r_1) = r_1$. Y listo, encontrado.

  Si no tuvimos tanta suerte podemos al menos saber que $GCD(b, r_1) = GCD(r_1, r_2)$, así que volvemos a aplicar el algoritmo de la división.

- Como los números encontrados satisfacen $0 \leq r_n < \cdots < r_2 < r_1$, vemos que este proceso terminar a lo mucho en b pasos, es decir para algún $n \leq b$ debemos tener que $r_n = 0$ y entonces:

$$\begin{aligned} GCD(a, b) &= GCD(b, r_1) \\ &= GCD(r_1, r_2) \\ &= \cdots \\ &= GCD(r_{n-2}, r_{n-1}) \\ &= GCD(r_{n-1}, 0) \\ &= r_{n-1} \end{aligned}$$

En otras palabras, el máximo común divisor de a, b es el último residuo distinto de cero al aplicar repetidamente el algoritmo de la división como en proceso anterior.

2.4.2. Ejemplo

Supón que tenemos que calcular el $GCD(2024, 748)$

- $GCD(2024, 748) = GCD(748, 528)$ donde $2024 = 748(2) + 528$
- $GCD(748, 528) = GCD(528, 220)$ donde $748 = 528(1) + 220$
- $GCD(528, 220) = GCD(220, 88)$ donde $528 = 220(2) + 88$
- $GCD(220, 88) = GCD(88, 44)$ donde $220 = 88(2) + 44$
- $GCD(88, 44) = GCD(44, 0) = 44$ donde $88 = 44(2) + 0$

Y bingo, 44.

2.4.3. Algorítmo Extendido de Euclides

Podemos añadir mas pasos al algoritmo de Euclides para darles más utilidad. Esta utilidad es casi exclusiva para encontrar los coeficientes de Bezout.

Ya idea básica esta en que podemos despejar los residuos de cada paso del algoritmo de Euclides original e ir sustituyendo cada uno de los residuos ya que podremos ir describiendo cada uno como una combinación lineal de a, b, cuando llegemos al último residuo, donde será cero, bastare con buscar la combinación anterior para encontrar las m, n.

Recuerda que la Identidad de Bezut nos dice que:

$$GCD(a, b) = am + bn \quad \text{donde} m, n \in \mathbb{Z} \tag{2.6}$$

Conocemos a m, n como los coeficientes de Bezut.

Demostración:

Supongamos que después de $n + 1$ pasos del algoritmo de Euclides llegamos que $r_{n+1} = 0$.

Eso nos dice que $r_n = GCD(a, b)$. Después de todo, eso es todo lo que se trata el algoritmo de Euclides.

Recuerda que $GCD(a, b) = GCD(b, r_1) = GCD(r_1, r_2)$ y así seguimos hasta que $GCD(r_{n-2}, r_{n-1}) = GCD(r_{n-1}, r_n) = GCD(r_n, 0) = r_n$

Recuerda que $a = bq + r$, es decir $r = a - bq$, pero recuerda que vimos que $b_n = r_{n-1}$, que $a_n = r_{n-2}$ por lo tanto vemos que $r_n = a - r_{n-1}q_n$ que es lo mismo que $r_n = r_{n-2} - r_{n-1}q_n$.

Ests fórmula es muy importante, así que la voy a repetir $r_n = r_{n-2} - r_{n-1}q_n$.

Ok, ahora con la fórmula lista podemos en vez de hacerlo para r_n hacerlo para r_{n-1}, donde vemos que $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$.

Ahora sustituyamos en la original:

$r_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n$
$r_n = (1 + q_nq_{n-1})r_{n-2} + (-q_n)r_{n-3}$

Si te das cuenta lo que hemos hecho es poner a r_n, es decir el GCD como una combinación lineal de los dos anteriores, y tu sabemos que si sigo aplicando este proceso hasta que r_n que descrito como combinación lineal de las r originales, es decir a, b.

2.4.4. Ejemplo

Supón que tenemos que calcular el $GCD(2024, 748)$ y también los coeficientes de Bezout.

Primero con el GCD, es decir con el algoritmo tradicional tenemos que:

- $GCD(2024, 748) = GCD(748, 528)$ donde $2024 = 748(2) + 528$
- $GCD(748, 528) = GCD(528, 220)$ donde $748 = 528(1) + 220$
- $GCD(528, 220) = GCD(220, 88)$ donde $528 = 220(2) + 88$
- $GCD(220, 88) = GCD(88, 44)$ donde $220 = 88(2) + 44$
- $GCD(88, 44) = GCD(44, 0) = 44$ donde $88 = 44(2) + 0$

Y bingo, 44.

Ahora vayamos haciendo las combinaciones lineales, ten en cuenta que muchas veces hacen el algoritmo extendido empezando por el último paso, hasta llegar a a, b, pero yo lo haré "al réves" empezando por a, b para llegar a $GCD(a, b)$, verás que lo entiendes mejor:

- Empecemos por mostrar a los originales a, b como combinación lineal de ellos:
  $2024 = 2024(1) + 748(0)$
  $748 = 2024(0) + 748(1)$
- Ahora podemos describir el primer paso del algoritmo como:
  $r = a - bq = 528 = 2024 - 748(2)$
  Y ahora sustituimos:
  $528 = 2024(1) + 748(-2)$
- Y lo hacemos para el segundo paso:
  $r = a - bq = 220 = 748 - 528(1)$
  Y ahora sustituimos:
  $220 = (2024(0) + 748(1)) - (2024(-1) + 748(-2)) = 2024(-1) + 748(3)$
- Y lo hacemos para el tercer paso:
  $r = a - bq = 88 = 528 - 220(2)$
  Y ahora sustituimos:
  $88 = (2024(1) + 748(-2)) - 2(2024(-1) + 748(3)) = 2024(3) + 748(-8)$
- Y lo hacemos para el cuarto paso:
  $r = a - bq = 44 = 220 - 88(2)$
  Y ahora sustituimos:
  $44 = (2024(-1) + 748(3)) - 2(2024(3) + 748(-8)) = 2024(-7) + 748(19)$
  Ahora llegamos a lo que queriamos

Bingo $44 = 2024(-7) + 748(19)$

2.5. Mínimo Común Múltiplo: MCM/LCM

Definición Formal

Dados dos números cualquiera $a, b \in \mathbb{Z} - \{0\}$.

Decimos que c es un múltiplo común de a, b si y solo si $a|c$ y $b|c$, es decir, si y solo si $\frac{c}{a}$ y $\frac{c}{b} \in \mathbb{Z}$.

Consideramos al mínimo común múltiplo como la mínima $c \in \mathbb{N}$ que cumple con ser un múltiplo común.

Ideas:

Si $ab \neq 0$, el conjunto múltiplos comunes positivos es distinto del vacío y por lo tanto tiene un elemento mínimo. Este elemento es llamado el mínimo común múltiplo de a y b. Este es denotado por $MCM(a, b) = LCM(a, b)$.

2.5.1. Propiedades de MCM/LCM

- Siempre se cumple que $GCD(a,b) \cdot LCM(a,b) = |ab|$

  Demostración:

  Sea $d = GCD(a,b)$ y $m = LCM(a,b)$.

  Entonces $d|a$ (digo es un divisor), entonces $d|ak$, digamos que $k = b$, entonces $d|ab$, es decir, $\frac{ab}{d} \in \mathbb{Z}$.

  Llamemos m' a $\frac{ab}{d}$ ya que se parece al máximo común multiplo.

  Veamos que $a|\frac{ab}{d}$, que es lo mismo que decir $\frac{\frac{ab}{d}}{a} = \frac{\frac{ab}{d}}{\frac{a}{1}}$ simplificando tenemos que $\frac{ab}{ad} = \frac{b}{d} \in \mathbb{Z}$. Esta oración debe ser verdadera pues, sabemos que $d|b$, por lo tanto $\frac{b}{d} \in \mathbb{Z}$. Es decir m' es un multiplo de a.

  Podemos ver que algo parecido pasa con b, preguntar si $b|\frac{ab}{d}$ es lo mismo que preguntar si $\frac{\frac{ab}{d}}{b} = \frac{\frac{ab}{d}}{\frac{b}{1}}$ simplicando tenemos que $\frac{ab}{db} = \frac{a}{d} \in \mathbb{Z}$. Esta oración debe ser verdadera pues, sabemos que $d|a$, por lo tanto $\frac{a}{d} \in \mathbb{Z}$. Es decir m' es un multiplo de b.

  Por lo tanto $m' \leq m$, es decir o m' es el mínimo común multiplo o es mayor que el. Podemos expresar lo anterior también como $\frac{ab}{d} \geq m = ab \geq md$.

  Por otro lado tenemos que por la identidad de Bezout $d = ax + by$, además sabemos que $m = as$ y $m = bt$

  Por lo que tenemos que $dm = (ax + by)m = axm + bym = ax(bt) + by(as) = ab(xt + ys)$ llamemos $k = (xt + ys)$, por lo que tenemos que $dm = ab(k)$, es decir $ab|dm$ y entonces recuerda que tenemos de las propiedades de divisibilidad que $|ab| \leq |dm|$, d, m son siempre positivos, así que $|ab| \leq dm$.

  Así que tenemos que $ab \geq md$, que es lo mismo que $|ab| \geq md$ y tenemos que $|ab| \leq dm$. Por lo tanto $ab = dm$.

  Esta identidad es endemoniadamente útil, prueba por ejemplo con: $GCD(12,-30) \cdot LCM(12,-30) = |(-12)(30)|$

- Si $LCM(a,b) = |ab|$ implica que $(a,b) = 1$

  Demostración:

  Si $LCM(a,b) = |ab|$ recuerda que $GCD(a,b) \cdot LCM(a,b) = |ab|$ Entonces $GCD(a,b) = \frac{|ab|}{LCM(a,b)}$ que ya dijimos que $GCD(a,b) = \frac{|ab|}{|ab|} = 1$.

2.6. Ecuaciones Diofanticas

Diofantos fue un matemático que vivió en Alexandria al rededor de 250 a.c. Él fue el primero en estudiar soluciones a ecuaciones del tipo $ax + by = c$ en los enteros.

Esa es la única razón por las que las llamamos así, esto es todo amiguitos.

Definición Formal

Una ecuación diofantinas es una ecuación del a forma $ax + by = c$ con $a, b, c \in \mathbb{Z}$.

Una solución de esta ecuación es un par de enteros x_0, y_0 que satisfacen la ecuación.

2.6.1. Soluciones

La ecuación $ax + by = c$ tiene solución si y sólo si, $GCD(a, b)|c$, es decir si $\frac{c}{GCD(a,b)}$.

Demostración:

En efecto, habíamos visto que un corolario de la demostración la identidad de Bezut, es que $Combinaciones = \{am + bn \mid m, n \in \mathbb{Z},\ am + bn > 0\}$. es precisamente el conjunto de múltiplos de $GCD(a, b)$.

Ahora sabemos que d es el menor elemento de ese conjunto, y más aún, que gracias a ese colorario que d divide a cualquier elemento del conjunto.

2.6.2. Soluciones Generales

Supón que x_0, y_0 es **una** solución a la ecuación $ax + by = c$, entonces todas las demás soluciones estarán dadas por:

- $x = x_0 + \frac{b}{d}t$
- $y = y_0 - \frac{a}{d}t$

Donde $t \in \mathbb{Z}$ y $d = GCD(a, b)$

Demostración:

Recuerda, ya sabemos que $ax_0 + by_0 = c$, ahora pongamos las soluciones generales de regreso $ax_0 + by_0 = c = ax + by$.

Podemos entonces ver que con Algebra llegaremos a que o bien $ax_0 + by_0 = ax + by$ o a algo mucho más interesante:

$a(x - x_0) = b(y_0 - y)$.

Ahora recuerda que ya habíamos probado que si $d = GCD(a, b)$. La pareja de $\frac{a}{d}, \frac{b}{d}$ siempre son primos relativos. Ya que escribir esas fracciones se ve feo pongamos que $r = \frac{a}{d}$ y $s = \frac{b}{d}$.

Pasa algo muy divertido si intentamos dividir entre d todo esto: $a(x - x_0) = b(y_0 - y)$ se convierte en $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$, que es lo mismo que:

$r(x - x_0) = s(y_0 - y)$

Bajo esa ecuación puede ver que $s(y_0 - y) = rq$, donde $q = (x - x_0)$ y $b = (y_0 - y)$ por lo tanto $r|sb$, ahora veamos que $GCD(r, s) = 1$ y que ya sabemos que $r|sb$ podemos aplicar un teorema que ya vimos antes que dice que "Supón $GCD(a, b) = 1$ y que $a|bc$, entonces $a|c$". Y afirmar con ello que $r|b$, es decir:

$r|(y_0 - y)$

Esto es lo mismo que decir que $(y_0 - y) = rt$, podemos despejar a y y tener que $y = y_0 - rt = y_0 - \frac{a}{GCD(a,b)}t$.

Ahora hagamos algo parecido con x, recordemos que $r(x - x_0) = s(y_0 - y)$

Bajo esa ecuación puede ver que $sq = r(x - x_0)$, donde $q = (y_0 - y)$ y $b = (x_0 - x)$ por lo tanto $s|rb$, ahora veamos que $GCD(r, s) = 1$ y que ya sabemos que $s|rb$ podemos aplicar un teorema que ya vimos antes que dice que "Supón $GCD(a, b) = 1$ y que $a|bc$, entonces $a|c$". Y afirmar con ello que $s|b$, es decir:

$s|(x - x_0)$

Esto es lo mismo que decir que $(x - x_0) = st$, podemos despejar a x y tener que $x = x_0 + st = x_0 + \frac{b}{GCD(a,b)}t$.

2.7. Función Phi de Euler: ϕ

Para un número $n \in \mathbb{N}$ tenemos que:

$$\phi(n) = Card(\{x \in \mathbb{N} \mid GCD(n, x) = 1 \text{ y además } x \leq n\}) \tag{2.7}$$

Es decir, $\phi(n)$ es la cantidad de naturales que son menores o iguales a n y que ademas son primos relativos.

2.7.1. Ejemplo

Supón que $n = 9$ entonces tenemos que:

- $GCD(1, 9) = 1$
- $GCD(2, 9) = 1$
- $GCD(3, 9) = 3$
- $GCD(4, 9) = 1$
- $GCD(5, 9) = 1$
- $GCD(6, 9) = 3$
- $GCD(7, 9) = 1$
- $GCD(8, 9) = 1$
- $GCD(9, 9) = 9$

Si te das cuenta los primos relativos de 9 son $1, 2, 4, 5, 7, 8$ por lo tanto $\phi(9) = 6$

2.7.2. Proposiciones Importantes

- Si $k > 1$ entonces $\phi(k) < k$

  Demostración:

  Si $\phi(1)$ entonces $GCD(1, 1) = 1$, por lo tanto $\phi(1) = 1$.

  En otro caso sabemos que $GCD(k, k) = k$ por lo tanto es imposible que $\phi(k) = k$, así que $\phi(k) < k$

- $\phi(p) = p - 1$ si y solo si p es primo

  Demostración:

  Si p es un número primo, entonces cada entero menor que p es primo relativo con con p, así que $\phi(p) = p - 1$.

  Por otro lado si $p > 1$ y $\phi(p) = p - 1$ entonces p tiene que ser primo pues de lo contrario p tiene un divisor d tal que $1 < d < p$ y entonces $\phi(n) \leq n - 2$.

Capítulo 3

Números Primos

3.1. Definición

Definición Formal

Un número $p \in \mathbb{N}$ es llamado número primo o simplemente primo, **si sus únicos divisores positivos son 1 y p**.

Un entero mayor que 1 que no es primo es llamado compuesto.

3.2. Proposiciones Importantes

- **Teorema de Euclides**: Si p es un primo y $p|ab$ entonces eso implica que p divide mínimo a a ó a b, es decir $p|a \vee p|b$

  Demostración:

  Esta es más fácil de lo que te imaginas, recuerda que si $GCD(a,b) = 1$ y que $a|bc$, entonces $a|c$.

  Ahora supongamos que $GCD(p,a) = 1$, es decir, que son primos relativos, y si sabemos aparte que $p|ab$ entonces $p|b$.

  Por el otro lado si $GCD(p,a) \neq 1$ entonces existe un multiplo común entre ellos y ya que p es primo, tenemos que $a = kp$ por lo tanto $p|a$.

- Hay una cantidad infinita de primos ($|\,\mathbb{P}\,| = \infty$)

  Demostración - Euclides Edition:

  Este también es un resultado muy famoso e importante, así que veamoslo con detalle:

  La demostración es por contradicción. Supongamos que sólo hay un número finito, Sean estos $MiniPrimos = \{p_1, p_2, \ldots, p_n\}$.

  Consideremos ahora el número $p' = p_1 \cdots p_n + 1$, pongamos esto como $p' = \prod_{n=1}^{n} p_k + 1$

  Tenemos dos opciones, o p es primo o p no lo es. (lo se, me merezco un Nobel).

  Pero p' no puede ser primo pues es más grande que todos los primos en la lista, así que si p' fuera un primo indicaría que nuestra lista esta incompleta.

  Si fuera compuesto entonces es divisible por algún primo. Digamos que ese primo se llama p_x, ahora supongamos que esta en el conjunto, eso indica que $p_x|p'$, que es lo mismo que poner $p_x|\prod_{n=1}^{n} p_k + 1$ y ya que p_x esta dentro del conjunto de $MiniPrimos$, entonces $p_x|\prod_{n=1}^{n} p_k$. Si te das cuenta usando un teorema anterior (Si $a|b$ y $a|b+c$ entonces $a|c$) tenemos que $p_x|1$ lo cual es imposible pues implicaría que $1 = kp_x$ y eso simplemente no se puede.

  Por lo tanto p_x no puede estar en $MiniPrimos$, así que el conjunto no esta completo.

  Si te das cuenta, sin importar que p' sea o no primo, la conclusión siempre es la misma, el conjunto no esta completo, hay más primos.

  Siempre hay más primos.

3.3. Como Saber si $n \in \mathbb{P}$

Dado un entero particular, ¿Cómo podemos saber si es primo o no?

Si el número es compuesto, ¿Cómo podemos encontrar un divisor no trivial?

3.3.1. Fuerza Bruta Inteligente

La primera idea es verificar si todos los enteros menores son divisores, si los únicos divisores son el 1 y el -1 entonces el número será primo.

Este método es simple pero costoso en términos de cómputo. Sin embargo hay una propiedad que nos podría facilitar el cálculo.

- Todo número compuesto n tiene un divisor a tal que $a \leq \sqrt{n}$

  Demostración:

  En efecto, como n es compuesto, $n = ab$.

  Si $a = b$, es decir si es un cuadrado perfecto entonces $a = b = a^2 = \sqrt{n}$.

  En caso contrario podemos suponer, que $a < b$, si multiplicamos por a tenemos que $a^2 < ab$. Por lo tanto $a^2 < n$. Por lo que $a < \sqrt{n}$.

3.4. Teorema Fundamental de la Aritmética

Un número $n \in \mathbb{N}$ puede ser expresado como un producto de primos.

Notese que dicha factorización es única si no cuentas el orden.

Demostración:

Parte I: Producto de Primos:

La demostración de la primera parte es mucho más sencilla de lo que parece:

Suponemos que $n \in \mathbb{N}$, si $n = 1$ entonces n es el producto de un conjunto vacío de primos.

Si $n \in \mathbb{P}$, osea si n es primo pues, pues ... Ya acabamos.

Si n no es primo entonces $n = ab$, y ahora en vez de enfocarnos en n lo hacemos en a, b.

Por inducción tenemos que llegar a que a, b es un primo o bien es el producto de dos naturales, y ahora analizamos a esos dos números... Si te das cuenta, es inducción y solo acaba cuando tanto a como b sean producto de primos.

Veríamos que por el principio de buen orden tenemos la secuencia que se nos va formando $1 < a < b < n$ y si siguieramos y cambiaramos nombre por consistencia $1 < \cdots < n_2 < n_1 < n$ tiene que terminar, no puede ser una lista y por ende un proceso infinito.

Por lo tanto n es siempre producto de Primos.

Parte II: Es Único:

Supongamos dos secuencias de primos que al multiplicarlos nos dan a n, incluso supongamos que existe la posibilidad de que sea diferente la cantidad de primos, esto estaría escrito como:

$n = p_1 p_2 p_3 \dots p_r = q_1 q_2 q_3 \dots q_s$ donde $r \leq s$

Ahora sabemos que n no es más que esas dos secuencias, por lo tanto $p_1 | n$, es decir $p_1 | q_1 q_2 q_3 \dots q_s$

El Teorema de Euclides (este: Si p es un primo y $p|ab$ entonces eso implica que p divide mínimo a a ó a b, es decir $p|a \vee p|b$) implica que o bien $p_1 = q_1$ ó bien $p_1 | q_2 q_3 \dots q_s$.

Así que por inducción veremos que $p_1 = q_i$ para alguna $1 \leq i \leq s$.

Entonces vemos que podemos cancelar a esa p_1 y a q_i y vemos que:

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

Repetimos este proceso de encontrar un compañero para alguna p_x r veces.

Si $r < s$ entonces $q_{r+1} \dots q_s = 1$ no es posible, por lo tanto $r = s$ y el conjunto de p_x y q_y son exactamente el mismo, hemos terminado la prueba. ¡Yeah!

3.4.1. Factorización Prima

Como vimos podemos escribir cualquier $n \in \mathbb{N}$ como:

$$n = p_1 p_2 p_3 \dots p_s \tag{3.1}$$

Estos p_i no tienen porque ser diferentes todos, así que otra forma equivalente de escribirlos es como:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \qquad \text{donde tenemos que } \alpha_i \geq 0, \text{ y también } p_1 < p_2 < \dots < p_r \tag{3.2}$$

Capítulo 4

Algoritmos Útiles

4.1. Exponenciación Binaria

Este es un algoritmo que te permite multiplicar más rápido, literalmente, ese es su objetivo, se basa en que si tiene un número como b^e y quieres calcularlo en vez de multiplicar b e veces, puedes ocupar la exponenciación binaria, que se basa en la observación de que:

$$\begin{aligned} \text{Si n es inpar: } b^e &= b(b^2)^{\frac{e-1}{2}} \\ \text{Si n es par: } b^e &= b(b^2)^{\frac{e}{2}} \end{aligned} \tag{4.1}$$

Ahora usando esto podemos crear 2 métodos alternos:

Método 1

Este método es bastante sencillo:

- Inicializa tu respuesta a ser 0
- Convierte el exponente en base 2
- Para cada digito del exponente en base 2 (Iniciando con el más significativo):
  - Si es 1: Nueva Respuesta = Respuesta^2
  - Si es 0: Nueva Respuesta = Base * Respuesta^2

Ejemplo Método 1

Este ejemplo nos muestra como usar esta propiedad para elevar más rápido, por ejemplo para encontrar x^{13} solo tenemos que seguir el algoritmo suponiendo que recuerdas que $13_{10} = 1101_2$:

Solución:

Inicializamos :	$respuesta = 1$	Ahora mismo: $respuesta = x^0$
Como 1^{er} dígito es 1:	$respuesta = respuesta^2 * x$	Ahora mismo: $respuesta = x^1$
Como 2^{do} dígito es 1:	$respuesta = respuesta^2 * x$	Ahora mismo: $respuesta = x^3$
Como 3^{er} dígito es 0:	$respuesta = respuesta^2$	Ahora mismo: $respuesta = x^6$
Como 4^{er} dígito es 1:	$respuesta = respuesta^2 * x$	Ahora mismo: $respuesta = x^13$

Método 2

Este método es bastante sencillo:

- Inicializa tu respuesta a ser 0
- Inicializa tu auxiliar a ser b
- Convierte el exponente en base 2
- Para cada digito del exponente en base 2 (Iniciando con el más significativo):
  - Si es 1: Nueva Respuesta = Respuesta * Auxiliar y Nuevo Auxiliar = Auxiliar^2
  - Si es 0: Nuevo Auxiliar = Auxiliar^2

Ejemplo Método 2

Este ejemplo nos muestra como usar esta propiedad para elevar más rápido, por ejemplo para encontrar x^{13} solo tenemos que seguir el algoritmo suponiendo que recuerdas que $13_{10} = 1101_2$:

Solución:

Inicializamos :	$res = 1$ y $aux = x$	Ahora: $res = x^0$ y $aux = x$
1^{er} dígito es 1:	$res = res * x$ y $aux = aux^2$	Ahora: $res = x^1$ y $aux = x^2$
2^{do} dígito es 0:	$aux = aux^2$	Ahora: $res = x^1$ y $aux = x^4$
3^{er} dígito es 1:	$res = res * x$ y $aux = aux^2$	Ahora: $res = x^5$ y $aux = x^8$
4^{er} dígito es 1:	$res = res * x$ y $aux = aux^2$	Ahora: $res = x^13$ y $aux = x^16$

Capítulo 5

Teoría de Congruencias

5.1. Congruencia Módulo N

Definición Formal

Si tenemos dos elementos $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$ entonces decirmos que a es **congruente** a b **modulo n** que escribimos como:

$$a \equiv b \pmod{n} \tag{5.1}$$

Si y solo si:

$$n|(a-b) \tag{5.2}$$

La idea principal de este nombre se da porque 2 enteros arbitrarios $a, b \in \mathbb{Z}$ son congruentes módulo n, esto es $a \equiv b \pmod{n}$, si y sólo si a y b dejan el mismo residuo al ser divididos por n. Esto lo demostraremos en las siguientes páginas.

5.1.1. Relación de Equivalencia

La notación $\equiv$ es usada porque las caracteristicas de la congruencia son muy muy parecidos a los de la igualdad ($=$), más exigentemente es porque es una relación de equivalencia.

- $a \equiv a \pmod{n}$

  Demostración:

  Sabemos que $n|0$ por lo tanto $n|a-a$, por lo tanto $a \equiv a \pmod{n}$

- Si $a \equiv b \pmod{n}$ entonces $b \equiv a \pmod{n}$

  Demostración:

  Si $a \equiv b \pmod{n}$ entonces $n|a-b$, por lo tanto $n|-(a-b)$, es decir $n|b-a$, por lo tanto $b \equiv a \pmod{n}$

- Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$ entonces $a \equiv c \pmod{n}$

  Demostración:

  Si $a \equiv b \pmod{n}$ entonces $n|a-b$ y si $b \equiv c \pmod{n}$ entonces $n|b-c$ (y recuerda que si $b|a$ y $b|c$ entonces $b|a \pm c$) por lo tanto $n|(a-b)+(b-c)$, es decir $n|a-b+b-c$, es decir $n|a-c$ por lo tanto $a \equiv c \pmod{n}$

5.1.2. Propiedades

- $a \equiv b \pmod{n}$ si y solo si $b \equiv a \pmod{n}$

  Demostración:

  Si $a \equiv b \pmod{n}$ entonces $n|a-b$, por lo tanto $n|-(a-b)$, es decir $n|b-a$, por lo tanto $b \equiv a \pmod{n}$

  Y Si $b \equiv a \pmod{n}$ entonces $n|b-a$, por lo tanto $n|-(b-a)$, es decir $n|a-b$, por lo tanto $a \equiv b \pmod{n}$

- Para cualesquiera dos enteros a, b son congruentes módulo 1

  Demostración:

  Esto es muy obvio pues $1|a-b$ (que es una proposición siempre verdadera) entonces $a \equiv b \pmod{1}$

- $a \equiv r \pmod{n}$ si y solo si podemos escribir a a como $a = nq + r$ para alguna q.

  Es decir, todo entero es congruente a su residuo r al ser dividido por n (módulo n).

  Otra forma común de encontrarlo es que $a = nq + b \Leftrightarrow a \equiv b \pmod{n}$

  Demostración:

  $a \equiv r \pmod{n}$ si y solo si $n|a-r$ que es lo mismo que decir $a - r = kn = nq$ que es lo mismo que decir $a = nq + r$.

- $a \equiv b \pmod{n}$, si y sólo si a y b dejan el mismo residuo al ser divididos por n.

  Demostración:

  $a \equiv b \pmod{n}$ si y solo si $a = nk + b$ para alguna k (es la proposición de arriba), despejemos $b = a - kn$.

  Ahora apliquemos el algoritmo de la división $a = nq + r$, con $0 < r < n$ sustituimos y tenemos que $b = nq + r - kn$ que es lo mismo que decir $b = n(q-k) + r$ con lo que podemos ver que dejan el mismo residuo al aplicar el algoritmo de la división con n.

- Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$ entonces $a + c \equiv b + d \pmod{n}$

  Demostración:

  Podemos escribir que $a = nq_1 + b$ y $c = nq_2 + d$ si las sumamos tenemos que: $a + c = nq_1 + nq_2 + b + d$ esto es lo mismo que $(a+c) = n(q_1+q_2) + (b+d)$ tenemos que $(a+c) - (b+d) = n(q_1+q_2)$, por lo tanto $n|(a+c) - (b+d)$, es decir $a + c \equiv b + d \pmod{n}$.

- Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$ entonces $ac \equiv bd \pmod{n}$

  Demostración:

  Podemos escribir que $a = nq_1 + b$ y $c = nq_2 + d$ si las multiplicamos tenemos que: $ac = (nq_1 + b)(nq_2 + d)$ esto es lo mismo que $(ac) = n^2 q_1 q_2 + dnq_1 + bnq_2 + bd$, por lo que tenemos que $(ac) = n(nq_1 q_2 + dq_1 + bq_2) + bd$, por lo tanto $(ac) - (bd) = n(nq_1 q_2 + dq_1 + bq_2)$ es decir $n|(ac) - (bd)$, es decir $ac \equiv bd \pmod{n}$.

5.1.3. Modulo: $A\,\%B$

Recuerda las 2 proposición demostrada allá arriba:

- $a, b \in \mathbb{Z}$ son congruentes módulo n, esto es $a \equiv b \pmod{n}$, si y sólo si a y b dejan el mismo residuo al ser divididos por n.
- $a \equiv r \pmod{n}$ si y solo si podemos escribir a a como $a = nq + r$ para alguna q.

Por esta razón el residuo de un número a cuando es divido por n (que es el mismo número el residuo que deja b al dividirlo entre n) lo solemos llamar $a\,\%b$.

Por lo tanto $a\,\%b = r$ donde $a = bq + r$ y $0 \leq r < b$.

5.2. Aplicaciones

5.2.1. Exponenciación Modular: $b^e \equiv s \pmod{n}$

Es muy común usar congruencias para encontrar el residuo s de un númerototote (generalmente denotado de la forma b^e) al divirlo entre alguna n, donde $0 \leq c < n$.

Usamos b de base, e de expontente y s de solución.

La idea se basa en la propiedad que ya demostramos de congruencias: "$a \equiv b \pmod{n}$ si y solo si ambos a, b dejan el mismo residio al ser dividido por n".

Este proceso, de encontrar s dado un número b^e y un módulo n es bastante fácil y rápido, incluso cuando el número es endemoniadamente grande, pero el proceso inverso, encontrar e dado una base b y un módulo n. Esto lo hace perfecto para la criptografía.

Forma 1:

- Aplica el algoritmo de la división y llega a $b = nq+r$, de aquí tienes la proposición $b \equiv r \pmod{n}$
- Empieza a elevar proposición anterior hasta llegar a:

  $b^k \equiv r^k \pmod{n}$ donde $r^k \equiv 1 \pmod{n}$
- Ya que sabemos que $1^n = 1$ entonces ya nos podremos acerca mucho más, ¿Pero cuanto?

  Aplica el algoritmo de la división y llega a $e = kq' + r'$, por lo tanto puedes escribir la proposición $b^{kq'} \equiv 1 \pmod{n}$
- Finalmente puedes también decir que $b^{r'} \equiv r^{r'} \pmod{n}$, por lo tanto si multiplicas las ultimas dos congruencias tenemos que $b^{kq'}b^{r'} \equiv (1)(r^{r'})$ esto es lo mismo que $b^{kq'+r'} \equiv r^{r'} \pmod{n}$

  Por lo tanto $b^e \equiv r^{r'} \pmod{n}$. Donde $r^{r'} \pmod{n}$ es nuestra respuesta.

Ejemplos

- Ejemplo 1: Encontrar el residuo de dividir 17^{341} entre 5

  Solución:

Sabemos que:	$17 \equiv 2$	(mód 5)
Por lo que:	$17^2 \equiv 2^2 = 4$	(mód 5)
y al cuadrado da:	$17^4 \equiv 4^2 = 16$	(mód 5)
y recuerda que:	$16 \equiv 1$	(mód 5)
por lo tanto:	$17^4 \equiv 1$	(mód 5)
y ya que $1^k = 1$:	$(17^4)^{85} = 7^{4*85} \equiv 1^{85} = 1$	(mód 5)
que es lo mismo que:	$17^{340} \equiv 1$	(mód 5)
y multiplicando por la 1^a congruencia:	$(17^{340})(17) \equiv 1(2)$	(mód 5)
que es lo mismo que:	$17^{341} \equiv 2$	(mód 5)

  Por lo tanto 17^{341} y 2 dejan el mismo residuo al divirlos entre 5

Capítulo 6

Grupos, Anillos y Campos

6.1. Grupo

Definición Formal

Un grupo es una combinación de tres elementos que van de la mano:

- **Conjunto Base:**

  Un conjunto llamado G que no este vacío (daaa!)

- **Relación Maestra:**

  Una relación entre $R : (G \times G) \to G$, es decir, es una relación que recibe dos elementos de G (o más específicos un par ordenado) y te regresa un nuevo elemento de G.

  Vamos a suponer que esta relación tendrá la misma notación que la multiplicación para que se vea mas normal: $(a)(b) = c$ donde $a, b, c \in G$

  Por lo tanto este grupo será cerrado con respecto a esa operación.

  Esta relación tiene que cumplir que sea asociativa, es decir $\forall a, b, c \in G,\ (ab)c = a(bc)$

- **Elemento Identidad para R:**

  Tendrá que existir un solo elemento llamado $1 \in G$ que cumpla con las siguientes caracteristicas:

  - **Es neutro con respecto a esa operación:** $\forall a \in G,\ 1a = a1 = a$
  - **Existen inversos:** $\forall a \in G,\ \exists b \in G,\ ab = ba = 1$

6.1.1. Grupo Abeliano

Un Grupo Abeliano es aquel grupo donde tenemos que:

$\forall a, b \in G,\ ab = ba$

6.2. Anillo

Definición Formal

Un Anillo es un conjunto G que viene equipado con dos relaciones R_1 y R_2, (la que me referiré con las notaciones de la suma y la multiplicación).

Donde se cumple que:

- G **es un grupo con respecto a** $+$
- G **es un grupo con respecto a** $*$
- **Propiedad Distrivutiva**

  Se cumple la propiedad especial en la que: $\forall a, b, c \in G,\ \ a(b+c) = ab + ac$