Algebra Superior 2

Grupo 4098

# Problemas Primer Parcial

**Alumnos:**

- 
- 
- 

**Profesor:**
Leonardo Faustinos Morales

**Ayudante:**
Jonathan López Ruiz

10 Octubre de 2017

# 1. Problemas

- 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.

- Muestre la identidad de Bezut $GCD(a,b) = am + bn$ donde $a = 25740$ y $b = 24633$:

  **Ejercicio**:

  Primero encontremos el GCD:

  - $(a : 25740) = (b : 24633)(q : 1) + (r : 1107)$
  - $(a : 24633) = (b : 1107)(q : 22) + (r : 279)$
  - $(a : 1107) = (b : 279)(q : 3) + (r : 270)$
  - $(a : 279) = (b : 270)(q : 1) + (r : 9)$
  - $(a : 270) = (b : 9)(q : 30) + (r : 0)$

  Ahora encontremos los coeficientes de Bezut:

  - $(a' : 25740) = (a' : 25740)(m : 1) + (b' : 24633)(n : 0)$
  - $(b' : 24633) = (a' : 25740)(m : 0) + (b' : 24633)(n : 1)$

  - $(r : 1107) = (a : 25740) - (b : 24633)(1 : 1) = (a' : 25740)(m : 1) + (b' : 24633)(n : -1)$
  - $(r : 279) = (a : 24633) - (b : 1107)(1 : 22) = (a' : 25740)(m : -22) + (b' : 24633)(n : 23)$
  - $(r : 270) = (a : 1107) - (b : 279)(1 : 3) = (a' : 25740)(m : 67) + (b' : 24633)(n : -70)$
  - $(r : 9) = (a : 279) - (b : 270)(1 : 1) = (a' : 25740)(m : -89) + (b' : 24633)(n : 93)$
  - $(r : 0) = (a : 270) - (b : 9)(1 : 30) = (a' : 25740)(m : 2737) + (b' : 24633)(n : -2860)$

  Por lo tanto tenemos que:

  - $GCD(25740, 24633) = 9$
  - Los coeficientes de Bezut son $-89, 93$

  Por lo tanto tenemos que: $(GCD : 9) = (a' : 25740)(m : -89) + (b' : 24633)(n : 93)$

- Resuelve $625x + 720y = 25$

  **Ejercicio**:

  Primero encontremos el GCD:

  - $(a : 625) = (b : 720)(q : 0) + (r : 625)$
  - $(a : 720) = (b : 625)(q : 1) + (r : 95)$
  - $(a : 625) = (b : 95)(q : 6) + (r : 55)$
  - $(a : 95) = (b : 55)(q : 1) + (r : 40)$
  - $(a : 55) = (b : 40)(q : 1) + (r : 15)$
  - $(a : 40) = (b : 15)(q : 2) + (r : 10)$
  - $(a : 15) = (b : 10)(q : 1) + (r : 5)$
  - $(a : 10) = (b : 5)(q : 2) + (r : 0)$

  Ahora encontremos los coeficientes de Bezut:

  - $(a' : 625) = (a' : 625)(m : 1) + (b' : 720)(n : 0)$
  - $(b' : 720) = (a' : 625)(m : 0) + (b' : 720)(n : 1)$

  - $(r : 625) = (a : 625) - (b : 720)(1 : 0) = (a' : 625)(m : 1) + (b' : 720)(n : 0)$
  - $(r : 95) = (a : 720) - (b : 625)(1 : 1) = (a' : 625)(m : -1) + (b' : 720)(n : 1)$
  - $(r : 55) = (a : 625) - (b : 95)(1 : 6) = (a' : 625)(m : 7) + (b' : 720)(n : -6)$
  - $(r : 40) = (a : 95) - (b : 55)(1 : 1) = (a' : 625)(m : -8) + (b' : 720)(n : 7)$
  - $(r : 15) = (a : 55) - (b : 40)(1 : 1) = (a' : 625)(m : 15) + (b' : 720)(n : -13)$
  - $(r : 10) = (a : 40) - (b : 15)(1 : 2) = (a' : 625)(m : -38) + (b' : 720)(n : 33)$
  - $(r : 5) = (a : 15) - (b : 10)(1 : 1) = (a' : 625)(m : 53) + (b' : 720)(n : -46)$
  - $(r : 0) = (a : 10) - (b : 5)(1 : 2) = (a' : 625)(m : -144) + (b' : 720)(n : 125)$

  Por lo tanto tenemos que:

  - $GCD(625, 720) = 5$
  - Los coeficientes de Bezut son $(53, -46)$

  Por lo tanto tenemos que: $(GCD : 5) = (a' : 625)(m : 53) + (b' : 720)(n : -46)$

  Ahora para llegar a la última basta con multiplicar por cinco, $5(GCD : 5) = 25 = (a' : 625)(m : 265) + (b' : 720)(n : -230)$

- Si $x, y$ son impares entonces $x^2 + y^2$ no puede ser un cuadrado perfecto

  **Demostración**:

  Esta demostración se deduce de manera inmediata del siguiente problema, pero ya que lo estoy haciendo en LaTeXes tal fácil como un copy paste :D

  Antes que nada recuerda que un cuadrado perfecto, lo podemos expresar como:

  - $(3k+0)^2 = 9k^2 = 3(3k^2)$
  - $(3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$
  - $(3k+2)^2 = 9k^2 + 12k + 3 + 1 = 3(3k^2 + 4k + 1) + 1$

  Es decir, todo cuadrado perfecto o es divisible entre 3 o es de la forma $3k+1$.

  Dado esto tenemos que:

$$\begin{aligned}(3k_1+1)^2 + (3k_2+1)^2 &= 9k_1^2 + 6k_1 + 1 + 9k_2^2 + 6k_2 + 1 \\ &= 9k_1^2 + 6k_1 + 9k_2^2 + 6k_2 + 2 \\ &= 9k_1^2 + 6k_1 + 9k_2^2 + 6k_2 + 2 \\ &= 3(3k_1^2 + 2k_1 + 3k_2^2 + 2k_2) + 2\end{aligned}$$

  Por lo tanto no puede ser un cuadrado perfecto.

- Sea $p$ un primo, si $p > 3$ y $p + 2$ es un primo también, entonces $12|2p + 2$

  **Demostración**:

  Para que a un número lo divida 12 tiene que ser divisible entre 4 y 3.

  Ahora como $p > 3$ entonces $p$ es impar, por lo tanto $p+1$ es par, además $2p+2$ es obviamente un par, por lo tanto, si $2p+2$ es par, y $2(p+1)$ es también par entonces $2p+2$ es divisible entre 4.

  Ahora como $p$ es primo y $p+2$ es primero entonces $p$ tiene que ser de la forma $3k+2$, por lo tanto $2p+2$ lo podemos poner como $6k+6$ es decir $3(2k+2)$ por lo tanto este número es divisible entre 3 también.

  Finalmente podemos concluir que $12|2p + 2$

- Un número $n \in \mathbb{Z}$ es divisible entre 4 si y solo si la suma de digitos (en base 10) de los últimos 2 digitos de $n$ es divisible entre 4.

  **Demostración**:

  Gracias a las congruencias podemos ver mcuho más fácil si un $n$ enorme es divisible.

  Antes que nada vamos a trabajar con los dígitos de $n$ como en base 10, así que antes vamos a explicar que son los dígitos siendo rigurosos matematicamente hablando:

$$\begin{aligned} n &= a_0(10^0) + a_1(10^1) + a_2(10^2) + \cdots + a_k(10^k) \\ n &= \sum_{i=0}^{k} a_i 10^i \qquad \text{con } 0 \leq a_i \leq 9 \end{aligned} \tag{1}$$

  Ahora, también recuerda que $4|10^k$ con $k < 1$. Para demostrar esto basta con ver que $100/4 = 25$, $1000/4 = 25$ (creo que la demostración formal por inducción es más que obvia, además todas las demás potencias base diez mayores son divisibles entre 100 y por transitividad también lo serán con 4), y para cualquier $k$ mayor se cumplirá, pero para $k = 0$ y $k = 1$, esto no es siempre cierto.

  Ahora $4|n$ si y solo si $n \equiv 0 \pmod 4$ y recuerda que podemos poner a $n$ escrito de otra forma: $a_0(10^0)+a_1(10^1)+a_2(10^2)+\cdots+a_k(10^k) \equiv 0 \pmod 4$ y como vimos por la propiedad anterior para potencias de 10 mayores que 1 tenemos que son congruentes con $0 \pmod 4$, por lo tanto la expresión de arriba se puede reducir a $4|n$ si y solo si: $a_0(10^0) + a_1(10^1) \equiv 0 \pmod 4$.

  Es decir si el el número formado por sus últimos 2 dígitos es divisible entre 4.

- Un número $n \in \mathbb{Z}$ es divisible entre 8 si y solo si la suma de digitos (en base 10) de los últimos 3 digitos de $n$ es divisible entre 8.

  **Demostración**:

  Antes que nada, recuerda que a $n$ lo puedes escribir como $n = a_0(10^0) + a_1(10^1) + a_2(10^2) + \cdots + a_k(10^k)$.

  Ahora, también recuerda que $8|10^k$ con $k < 2$. Para demostrar esto basta con ver que $1000/8 = 125$, $10000/8 = 1250$ (creo que la demostración formal por inducción es más que obvia), y para cualquier $k$ mayor se cumplirá, pero para $k = 0$, $k = 1$ o $k = 2$, esto no es siempre cierto.

  Ahora $8|n$ si y solo si $n \equiv 0 \pmod 8$ y recuerda que podemos poner a $n$ escrito de otra forma: $a_0(10^0)+a_1(10^1)+a_2(10^2)+\cdots+a_k(10^k) \equiv 0 \pmod 8$ y como vimos por la propiedad anterior para potencias de 10 mayores que 2 tenemos que son congruentes con $0 \pmod 8$, por lo tanto la expresión de arriba se puede reducir a $8|n$ si y solo si: $a_0(10^0) + a_1(10^1) + a_2(10^2) \equiv 0 \pmod 8$.

  Es decir si el el número formado por sus últimos 3 dígitos es divisible entre 8.

- Un primo de la forma $3k+1$ es de la forma $6k+1$

  **Demostración**:

  Sabemos que $p = 3k+1$ por lo tanto $p-1 = 3k$ es decir $p-1$ es divisible entre 3, por lo tanto $p-1 = 6k$. ¿Porque?

  Porque supongamos que $p-1 = 3k_0$ pero no $p-1 = 6k_1$ (osea $p-1 = 3(2k_1)$), por lo tanto tendrá que ser de la forma $p-1 = 3(2k_1+1)$ es decir impar, pero eso implicaría que $p$ sea par. Cosa que no puede ser.

  Así $p-1$ si es de la forma $p-1 = 6k$ por lo tanto $p = 6k+1$.

- Dado un conjunto de $k$ enteros arbitrarios diferentes (donde $k \in \mathbb{N}$ y $k > 1$ ) siempre se tiene que la diferencia de dos de ellos será divisible por $k$.

  **Demostración**:

  Sean $a_1, a_2, a_3, \ldots, a_{k+1}$ los $k$ enteros.

  Apliquemos el algoritmo de la división para todos los elementos del conjunto, obteniendo algo como:

  - $a_1 = b_1 + r_1$
  - $a_2 = b_2 + r_2$
  - $a_3 = b_3 + r_3$
  - $\ldots$

  Ahora, el truco esta en que como tenemos $k$ residuos, pero todos ellos tienen que cumplir que $0 \geq r_x < b$, pero esto implica que solo puede haber $k-1$ resudios posibles: $0, 1, \ldots, k-1$. Por lo tanto habrá dos residuos iguales.

  Tomemos ambos enteros que nos dan resudios iguales y saquemos la diferencia:

$$\begin{aligned}
a_i - a_j &= (bq_i + r_i) - (bq_j + r_j) \\
&= (bq_i + r_i) - (bq_j + r_i) \\
&= (bq_i + r_i) - bq_j - r_i) \\
&= bq_i - bq_j \\
&= b(q_i - q_j) + 0 \\
&= bq_x + 0
\end{aligned}$$

  Y bingo, demostrado ;)

- Si $2^k + 1$ es primo entonces $k = 2^n$

  **Demostración**:

  Ya que $k$ no es de la forma $2^n$ podemos decir que en su descomposición prima hay mínimo un factor impar, el único caso en el que no pasa esto es cuando $k = 2^n$ podemos decir entonces que $k = rs$ con $s$ impar.

  Ya que tenemos que $a - b | a^m - b^m$ entonces podemos decir que $(2^r - (-1)) | (2^r)^s - (-1)^s$, pero como $s$ es impar $(2^r - (-1)) | (2^r)^s - (-1)$, es decir $(2^r + 1) | 2^{rs} + 1$, es decir, por lo tanto $2^k + 1$ tiene un factor, el $(2^r + 1)$, por lo que no es primo.