Algebra Superior 2

Grupo 4098

Soluciones y Demostraciones

Alumnos:

- Palacios Rodríguez Ricardo Rubén
- Rosas Hernandez Oscar Andres
- José Martín Panting Magaña
- Raúl Leyva Cedillo
- Angel Mariano Guiño Flores
- Gloria Guadalupe Cervantes Vidal
- David Iván Morales Campos
- Aaron Barrera Tellez
- Elias Garcia Alejandro
- Víctor Hugo García Hernández
- Oscar Márquez Esquivel

Profesor:
Leonardo Faustinos Morales

12 de Septiembre de 2017

Índice

1. Divisibilidad

1.1. Problema 1

Algoritmo de Euclides: Encontrar el GCD(A, B)

Calcular el $GCD(2947, 3997)$

- $(a : 2947) = (b : 3997)(q : 0) + (r : 2947)$
- $(a : 3997) = (b : 2947)(q : 1) + (r : 1050)$
- $(a : 2947) = (b : 1050)(q : 2) + (r : 847)$
- $(a : 1050) = (b : 847)(q : 1) + (r : 203)$
- $(a : 847) = (b : 203)(q : 4) + (r : 35)$
- $(a : 203) = (b : 35)(q : 5) + (r : 28)$
- $(a : 35) = (b : 28)(q : 1) + (r : 7)$
- $(a : 28) = (b : 7)(q : 4) + (r : 0)$

Así que $GCD(2947, 3997) = 7$

Calcular el $GCD(2689, 4001)$

- $(a : 2689) = (b : 4001)(q : 0) + (r : 2689)$
- $(a : 4001) = (b : 2689)(q : 1) + (r : 1312)$
- $(a : 2689) = (b : 1312)(q : 2) + (r : 65)$
- $(a : 1312) = (b : 65)(q : 20) + (r : 12)$
- $(a : 65) = (b : 12)(q : 5) + (r : 5)$
- $(a : 12) = (b : 5)(q : 2) + (r : 2)$
- $(a : 5) = (b : 2)(q : 2) + (r : 1)$
- $(a : 2) = (b : 1)(q : 2) + (r : 0)$

Así que $GCD(2689, 4001) = 1$

Calcular el $GCD(7469, 2464)$

- $(a : 7469) = (b : 2464)(q : 3) + (r : 77)$
- $(a : 2464) = (b : 77)(q : 32) + (r : 0)$

Así que $GCD(7469, 2464) = 77$

Calcular el $GCD(2947, 3997)$

- $(a : 2947) = (b : 3997)(q : 0) + (r : 2947)$
- $(a : 3997) = (b : 2947)(q : 1) + (r : 1050)$
- $(a : 2947) = (b : 1050)(q : 2) + (r : 847)$
- $(a : 1050) = (b : 847)(q : 1) + (r : 203)$
- $(a : 847) = (b : 203)(q : 4) + (r : 35)$
- $(a : 203) = (b : 35)(q : 5) + (r : 28)$
- $(a : 35) = (b : 28)(q : 1) + (r : 7)$
- $(a : 28) = (b : 7)(q : 4) + (r : 0)$

Así que $GCD(2947, 3997) = 7$

Calcular el $GCD(1109, 4999)$

- $(a : 1109) = (b : 4999)(q : 0) + (r : 1109)$
- $(a : 4999) = (b : 1109)(q : 4) + (r : 563)$
- $(a : 1109) = (b : 563)(q : 1) + (r : 546)$
- $(a : 563) = (b : 546)(q : 1) + (r : 17)$
- $(a : 546) = (b : 17)(q : 32) + (r : 2)$
- $(a : 17) = (b : 2)(q : 8) + (r : 1)$
- $(a : 2) = (b : 1)(q : 2) + (r : 0)$

Así que $GCD(1109, 4999) = 1$

1.2. Problema 3

Algoritmo de Euclides Extendido y Coeficientes de Bezut

Encontremos los coeficientes de $243x + 198y = 9$

- $(a : 243) = (b : 198)(q : 1) + (r : 45)$
- $(a : 198) = (b : 45)(q : 4) + (r : 18)$
- $(a : 45) = (b : 18)(q : 2) + (r : 9)$
- $(a : 18) = (b : 9)(q : 2) + (r : 0)$

El proceso para encontrar los coeficientes de Bezut son:

- $(a' : 243) = (a' : 243)(m : 1) + (b' : 198)(n : 0)$
- $(b' : 198) = (a' : 243)(m : 0) + (b' : 198)(n : 1)$

- $(r : 45) = (a : 243) - (b : 198)(1 : 1) = (a' : 243)(m : 1) + (b' : 198)(n : -1)$
- $(r : 18) = (a : 198) - (b : 45)(1 : 4) = (a' : 243)(m : -4) + (b' : 198)(n : 5)$
- $(r : 9) = (a : 45) - (b : 18)(1 : 2) = (a' : 243)(m : 9) + (b' : 198)(n : -11)$
- $(r : 0) = (a : 18) - (b : 9)(1 : 2) = (a' : 243)(m : -22) + (b' : 198)(n : 27)$

Por lo tanto el $GCD(243, 198) = 9$
Y los números de Bezut son $(243, 198) = (9, -11)$
Y la Identidad de Bezut es: $(GCD : 9) = (a' : 243)(m : 9) + (b' : 198)(n : -11)$

Encontremos los coeficientes de $71x + 50y = 1$

- $(a : 71) = (b : 50)(q : 1) + (r : 21)$
- $(a : 50) = (b : 21)(q : 2) + (r : 8)$
- $(a : 21) = (b : 8)(q : 2) + (r : 5)$
- $(a : 8) = (b : 5)(q : 1) + (r : 3)$
- $(a : 5) = (b : 3)(q : 1) + (r : 2)$
- $(a : 3) = (b : 2)(q : 1) + (r : 1)$
- $(a : 2) = (b : 1)(q : 2) + (r : 0)$

El proceso para encontrar los coeficientes de Bezut son:

- $(a' : 71) = (a' : 71)(m : 1) + (b' : 50)(n : 0)$
- $(b' : 50) = (a' : 71)(m : 0) + (b' : 50)(n : 1)$

- $(r : 21) = (a : 71) - (b : 50)(1 : 1) = (a' : 71)(m : 1) + (b' : 50)(n : -1)$
- $(r : 8) = (a : 50) - (b : 21)(1 : 2) = (a' : 71)(m : -2) + (b' : 50)(n : 3)$
- $(r : 5) = (a : 21) - (b : 8)(1 : 2) = (a' : 71)(m : 5) + (b' : 50)(n : -7)$
- $(r : 3) = (a : 8) - (b : 5)(1 : 1) = (a' : 71)(m : -7) + (b' : 50)(n : 10)$
- $(r : 2) = (a : 5) - (b : 3)(1 : 1) = (a' : 71)(m : 12) + (b' : 50)(n : -17)$
- $(r : 1) = (a : 3) - (b : 2)(1 : 1) = (a' : 71)(m : -19) + (b' : 50)(n : 27)$
- $(r : 0) = (a : 2) - (b : 1)(1 : 2) = (a' : 71)(m : 50) + (b' : 50)(n : -71)$

Por lo tanto el $GCD(71, 50) = 1$
Y los números de Bezut son $(71, 50) = (-19, 27)$
Y la Identidad de Bezut es: $(GCD : 9) = (GCD : 1) = (a' : 71)(m : -19) + (b' : 50)(n : 27)$

Encontremos los coeficientes de $43 + 64 = 1$

- $(a : 43) = (b : 64)(q : 0) + (r : 43)$
- $(a : 64) = (b : 43)(q : 1) + (r : 21)$
- $(a : 43) = (b : 21)(q : 2) + (r : 1)$
- $(a : 21) = (b : 1)(q : 21) + (r : 0)$

El proceso para encontrar los coeficientes de Bezut son:

- $(a' : 43) = (a' : 43)(m : 1) + (b' : 64)(n : 0)$
- $(b' : 64) = (a' : 43)(m : 0) + (b' : 64)(n : 1)$

- $(r : 43) = (a : 43) - (b : 64)(1 : 0) = (a' : 43)(m : 1) + (b' : 64)(n : 0)$
- $(r : 21) = (a : 64) - (b : 43)(1 : 1) = (a' : 43)(m : -1) + (b' : 64)(n : 1)$
- $(r : 1) = (a : 43) - (b : 21)(1 : 2) = (a' : 43)(m : 3) + (b' : 64)(n : -2)$
- $(r : 0) = (a : 21) - (b : 1)(1 : 21) = (a' : 43)(m : -64) + (b' : 64)(n : 43)$

Por lo tanto el $GCD(43, 64) = 1$
Y los números de Bezut son $(43, 64) = (3, -2)$
Y la Identidad de Bezut es: $(GCD : 1) = (a' : 43)(m : 3) + (b' : 64)(n : -2)$

Encontremos los coeficientes de $93 + 81 = 3$

- $(a : 93) = (b : 81)(q : 1) + (r : 12)$
- $(a : 81) = (b : 12)(q : 6) + (r : 9)$
- $(a : 12) = (b : 9)(q : 1) + (r : 3)$
- $(a : 9) = (b : 3)(q : 3) + (r : 0)$

El proceso para encontrar los coeficientes de Bezut son:

- $(a' : 93) = (a' : 93)(m : 1) + (b' : 81)(n : 0)$
- $(b' : 81) = (a' : 93)(m : 0) + (b' : 81)(n : 1)$

- $(r : 12) = (a : 93) - (b : 81)(1 : 1) = (a' : 93)(m : 1) + (b' : 81)(n : -1)$
- $(r : 9) = (a : 81) - (b : 12)(1 : 6) = (a' : 93)(m : -6) + (b' : 81)(n : 7)$
- $(r : 3) = (a : 12) - (b : 9)(1 : 1) = (a' : 93)(m : 7) + (b' : 81)(n : -8)$
- $(r : 0) = (a : 9) - (b : 3)(1 : 3) = (a' : 93)(m : -27) + (b' : 81)(n : 31)$

Por lo tanto el $GCD(93, 81) = 3$
Y los números de Bezut son $(93, 81) = (7, -8)$
Y la Identidad de Bezut es: $(GCD : 3) = (a' : 93)(m : 7) + (b' : 81)(n : -8)$

Encontremos los coeficientes de $10x + 15y = 5$ ... Espera, este es muy obvio, es simplemente $(GCD : 5) = (a' : 10)(m : -1) + (b' : 15)(n : 1)$

Mientras que el de $6x + 5y = 1$ es $(GCD : 1) = (a' : 6)(m : 1) + (b' : 5)(n : -1)$

Por lo tanto: $(GCD : 1) = (a' : 6)(m : 1) + (b' : 10)(n : 1) + (c' : 15)(o : -1)$

1.3. Problema 5

¿Cuantos enteros hay entre 100 y 1000 que sean divisibles entre 7?

Empecemos porque el primero es 105, de ahi hay 127 más, pues 105 + (127 * 7) = 994.

Por lo tanto son 128 enteros.

Otro truco es aplicar el algoritmo de la división y ver que $1000 = 7(142) + 6$ y $100 = 7(14) + 2$ y $142 - 14 = 128$.

1.4. Problema 7

Mostrar 3 enteros que son relativos, pero no primos relativos a pares

Esto simplemente no se puede, si un conjunto es primo relativo, entonces lo será cada par de sus elementos.

1.5. Problema 9

Si $bc|ac$ entonces $a|c$

Demostración:

Si $c = 0$ esto se reduce a $0|0$ lo cual es cierto.

Si $bc|ac$ entonces $ac = q(bc)$, por lo tanto ya que estamos en los enteros podemos cancelar y ver que $a = bq$ es decir $b|a$.

1.6. Problema 11

Nunca se cumple que $4|n^2 + 2$

Demostración:

Suponga que n es par, por lo tanto tenemos que: $(2k)^2 + 2$ se puede expresar como $4k^2 + 2$, por lo tanto no es divisible entre cuatro.

Si n es impar, tenemos que $(2k+1)^+2$ se puede expresar como $4k^2+4k+1+2$ es decir $4(k^2+k)+3$, por lo tanto tampoco es divisible entre cuatro.

1.7. Problema 13

Si k es primo entonces el producto de todos los primos menores o iguales que k divide a $n^k - n$

Demostración:

Suponga que k es primo, por lo tanto si $k = 2$ tenemos que $(n^2 - n) = n(n-1)$ y como son dos números consecutivos mínimo uno es par. Por lo tanto $2|n^2 - n$.

Si $k \neq 2$ entonces k es impar, veamos que pasa con los primos primos:

Si $k = 3$ entonces $(n^3 - n) = n(n+1)(n-1)$ es decir 3 números consecutivos por lo tanto es divisible entre 3 y también entre 2. Por lo tanto $2 * 3|n^3 - n$.

Si $k = 5$ entonces:

$$\begin{aligned}
(n^5 - n) &= n(n^4 - 1) \\
&= n(n^2 + 1)(n^2 - 1) \\
&= n(n+1)(n-1)(n^2 + 1) \\
&= n(n+1)(n-1)(n-2)(n+2) + 5
\end{aligned}$$

es decir son 5 números consecutivos por lo tanto es divisible entre 5, 3 y también entre 2. Por lo tanto $2 * 3 * 5|n^5 - n$.

De forma más general como $k - 1$ es par y tenemos la expresión $n(n^k - 1)$ donde podemos expandir este polinomio para tener k números consecutivos (esto se prueba usando inducción) es decir, será divisible entre el producto de los primos menores o iguales que k.

1.8. Problema 15

Si x, y son impares entonces $(x^2 + y^2)$ es par pero no divisible entre 4

Demostración:

Pongamos que: $x = 2k_1 + 1$ y $x = 2k_2 + 1$, entonces:

$$\begin{aligned}
x^2 + y^2 &= (2k_1 + 1)^2 + (2k_2 + 1)^2 \\
&= 4k_1^2 + 4k_1 + 1 + 4k_2^2 + 4k_2 + 1 \\
&= 4k_1^2 + 4k_1 + 4k_2^2 + 4k_2 + 2 \\
&= 4(k_1^2 + k_1 + k_2^2 + k_2) + 2 \\
&= 2(2(k_1^2 + k_1 + k_2^2 + k_2) + 1)
\end{aligned}$$

Gracias a la última línea vemos que que $x^2 + y^2$ es par, y gracias a la penúltima línea es vemos que no puede ser divisible entre 4

1.9. Problema 17

$GCD(n, n+1) = 1$

Demostración:

Sea $d = GCD(n, n+1)$, ahora tenemos que $d|n$ y $d|n+1$, por lo tanto divide a cualquier combinación lineal como por ejemplo $d|(-1)n + 1(n+1)$ entonces $d|1$ por lo tanto solo le queda a d ser uno.

1.10. Problema 17.1

$LCM(n, n+1) = |n(n+1)|$

Demostración:

Ya sabemos que $GCD(n, n+1) = 1$ por lo tanto $(1)LCM(n, n+1) = |n(n+1)|$

1.11. Problema 19

Cualquier conjunto de números primos a pares, son primos relativos

Demostración:

Por contradicción, supón que hay un conjunto donde no son primos relativos, pero si sus pares de elementos son coprimos.

Sabemos que:

$$A = \{\ a_1, a_2, a_3, \ldots, a_{n-1}, a_n\ \} \text{ donde } (a_i, a_j) = 1\ \forall i, j,\ \ i \neq j$$

Si el conjunto no fuera coprimo entonces pasaría que: $GCD(a_1, a_2, a_3, \ldots, a_{n-1}, a_n) = d$ con $d \neq 1$

Y por definición sabemos que $d|a_i\ \forall a_i \in S$

Pero si para todos los pares de números tenemos que el único número que divide a ambos es el uno.

Así, ningún miembro de A tiene un divisor común con d lo que sea una contradicción.

Por lo tanto, el conjunto de enteros que son relativamente primos en pares es también relativamente primo.

1.12. Problema 21

Demuestre que cualquier entero de la forma $6k+5$ es de la forma $3k-1$ pero no de manera inversa

Demostración:

Si tenemos un número de la forma $6k+5$ entonces ve que $6k+5 = 3(2k+2) - 1$

Pero veamos una contraprueba para su inversa: Dado un número de la forma $3k-1$, por ejemplo 3, tenemos el $3(3) - 1 = 8$ no lo podemos escribir de la forma $6k+5$, pues implica $6k+5 = 8$ es decir $6k = 3$, lo cual obviamente no tiene solución en los enteros, por lo tanto queda demostrado que su inversa no es correcta.

1.13. Problema 23

$n^2 = 3k$ ó $n^2 = 3k+1$

Demostración:

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 $3k+1$.

1.14. Problema 25

Demuestre que existe una cantidad infinita de enteros x, y tal que $x+y = 100$ y $(x,y) = 5$

Demostración:

Ve que una solución es $55 + 45 = 5$ y $(55, 45) = 5$ Para encontrar todas las demás soluciones simplemente tenemos que:

- x = 55 + r
- y = 45 - r

donde $r = 100k$ y k es cualquier entero tal que $(k, 55) = 1$

1.15. Problema 27

Encuentre los enteros que cumple con que $(a, b) = 10$ y $[a, b] = 100$

Demostración:

Empecemos por enunciar a más detalle las restricciones que nos estan dando como $(a, b) = 10$, entonces tenemos que $10|a$ y $10|b$ por lo tanto $10 \leq a, b$.

Y como $[a, b] = 100$ entonces $a|100$ y $b|100$, por lo tanto $a, b \leq 100$.

Con lo cual sabemos que dichos enteros tiene que estar entre 10 y 100, ahora podemos ocupar que $(a, b) = 10$ y ver que tenemos que:

$a = 10q_1$ y $b = 10q_2$ con $(q_1, q_2) = 1$.

Ademas $(a, b)[a, b] = 1000$. Por lo tanto dichas parejas son:

- $(100, 10)$
- $(20, 50)$

1.16. Problema 29

$a, b \in \mathbb{Z}$ existen enteros x, y tal que $GCD(x, y) = b$ y $LCM(x, y) = a$ si y solo si $b|a$

Demostración:

Probemos por doble condicional.

Empecemos de ida:

Dado $GCD(x, y) = b$ por lo tanto $b|x$ y dado $LCM(x, y) = a$ por lo tanto $x|a$ y ya que la divisibilidad es transicitva tenemos por lo tanto que $b|a$.

Ahora de regreso regreso:

Si $b|a$, entonces $a = bq$. Podemos decir que $GCD(b, a) = GCD(b, bq) = b \cdot GCD(1, q)$. Podemos decir que $MCL(b, a) = MCL(b, bq) = bq = a$.

Por lo tanto propongamos que $x = a$ y a $y = b$ entonces tenemos que se cumple la propiedad.

1.17. Problema 31

$a - b|a^n - b^n$

Demostración:

Para que fuera cierto teniamos que encontrar $a^n - b^n = a - b(q)$ podemos proponer de manera completamente arbitraria que:

$$\begin{aligned}(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} &= (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} \\ &= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k} \\ &= a^n + \sum_{k=1}^{n-1} a^k b^{n-k} - \sum_{k=1}^{n-1} a^k b^{n-k} - b^n \\ &= a^n - b^n\end{aligned}$$

1.18. Problema 31.1

$a - 1|a^n - 1$

Ideas:

Es muy obvio esto si $n = 1$, pues $a - 1|a - 1$ y con $n = 2$, pues $a - 1|a^2 - 1$ ya que gracias a la diferencia de cuadrados tenemos que: $a - 1|(a + 1)(a - 1)$.

Con una n par es también muy fácil pues basta con ver que podemos siempre factorizar un $a-1$, pero también podemos hacer lo mismo con un n impar, basta con ver la descomposición del polinomio.

Demostracion:

Recuerdas la serie geométrica, sino no te preocupes, pues tenemos que:

$$a + ar + ar^2 + ar^3 + \cdots + ar^{n-1} = \sum_{k=0}^{n-1} ar^k = a\frac{1-r^n}{1-r} = a\frac{(-1)(r^n-1)}{(-1)r-1} = a\frac{r^n-1}{r-1}$$

Por lo tanto si pones a $a = 1$ y $r = a$ tienes que:

$$1 + a + a^2 + a^3 + \cdots + a^{n-1} = \sum_{k=0}^{n-1} a^k = \frac{1-a^n}{1-a} = \frac{(-1)(a^n-1)}{(-1)a-1} = \frac{a^n-1}{a-1}$$

Por lo tanto ya que solo estamos sumando enteros o potencias de enteros $\dfrac{a^n-1}{a-1}$ debe ser un entero, es decir $a - 1|a^n - 1$.

1.19. Problema 33

GCD(a,b,c) = GCD((a, b), c)

Demostración:

Usando la factorización de primos tenemos que:

- $a = \prod_i p^{\alpha_i}$
- $b = \prod_i p^{\beta_i}$
- $c = \prod_i p^{\gamma_i}$

Entonces tenemos que:

$$GCD(a,b,c) = \prod_i p^{min(\alpha_i,\beta_i,\gamma_i)} = \prod_i p^{min(min(\alpha_i,\beta_i),\gamma_i))} = GCD((a,b),c)$$

1.20. Problema 35

Si $GCD(b,c) = 1$ y $r|b$ entonces $GCD(r,c) = 1$

Demostración:

Usando la Identidad de Bezut esto esta regalado pues tenemos que $bx + cy = 1$ y $b = rq$ entonces $r(qx) + cy = 1$ por lo tanto $GCD(r,c) = 1$. Que facil son ciertas demostraciones.

2. Primos

2.1. Problema 2

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

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 $10 \equiv 1 \pmod{3}$.

Ahora $3|n$ si y solo si $n \equiv 0 \pmod{3}$ y recuerda que podemos poner a n escrito de otra forma: $a_0(10^0)+a_1(10^1)+a_2(10^2)+\cdots+a_k(10^k) \equiv 0 \pmod{3}$ y como recuerdas ($10 \equiv 1 \pmod{3}$) tenemos que esto ocurre si y solo si: $a_0+a_1+\cdots+a_k \equiv 0 \pmod{3}$, esto es lo mismo que $3|a_0+a_1+a_2+\ldots$.

Es decir, un número $n \in \mathbb{Z}$ es divisble entre 3 si y solo si la suma de digitos de n es divisible entre 3.

2.2. Problema 3

Cualquier número es divisible entre 11 si y solo si la diferencia de la suma de los dígitos impares y los dígitos pares son divisibles entre 11

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, veamos este curioso patrón donde esta la clave:

- $10 \equiv -1 \pmod{11}$
- $100 \equiv (10)(10) \equiv (-1)(-1) \equiv 1 \pmod{11}$
- $1000 \equiv (100)(10)(10) \equiv (-1)(-1)(-1) \equiv -1 \pmod{11}$
- $\ldots$

Por lo tanto vemos que que de manera general $10^n \equiv (-1)^n \pmod{11}$

Entonces si un número x es divisible entre 11 tendremos que $x \equiv 0 \pmod{11}$ Por lo tanto $(1)a_0 + (10)a_1 + \cdots + (10^k)a_k \equiv 0 \pmod{11}$ es decir $(1)a_0 + (-1)a_1 + (1)a_1 + \cdots + (-1)^{k-1}a_k \equiv 0 \pmod{11}$

Que si te das cuenta, es lo que queriamos demostrar :D

2.3. Problema 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 $p = 6k + 1$.

2.4. Problema 10

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.

2.5. Problema 11

Si x, y son coprimos con 3 entonces $x^2 + y^2$ no puede ser un cuadrado perfecto

Demostración:

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 $3k + 1$.

Veamos los casos posibles:

- $x = 3k_1 + 1$ y $y = 3k_2 + 1$
  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.
- $x = 3k_1 + 1$ y $y = 3k_2 + 2$
  Dado esto tenemos que:
  $$\begin{aligned}(3k_1+1)^2 + (3k_2+2)^2 &= 9k_1^2 + 6k_1 + 1 + 9k_2^2 + 12k_2 + 3 + 1\\ &= 9k_1^2 + 6k_1 + 3 + 9k_2^2 + 12k_2 + 2\\ &= 3(3k_1^2 + 2k_1 + 1 + 3k_2^2 + 4k_2) + 2\end{aligned}$$
  Por lo tanto no puede ser un cuadrado perfecto.
- $x = 3k_1 + 2$ y $y = 3k_2 + 2$
  Dado esto tenemos que:
  $$\begin{aligned}(3k_1+2)^2 + (3k_2+2)^2 &= 9k_1^2 + 12k_1 + 3 + 1 + 9k_2^2 + 12k_2 + 3 + 1\\ &= 9k_1^2 + 12k_1 + 6 + 9k_2^2 + 12k_2 + 2\\ &= 3(3k_1^2 + 6k_1 + 2 + 3k_2^2 + 6k_2) + 2\end{aligned}$$
  Por lo tanto no puede ser un cuadrado perfecto.

2.6. Problema 24.1

Si a, b son naturales diferentes entonces $(a, c) = (a, b)$ implica que $[a, b] \neq [a, c]$

Demostración:

Ahora, si fuera el caso tendriamos que: $(a, b)\ [a, b] = ab$ y $(a, c)\ [a, c] = ac$ por lo tanto $ac = ab$ pero dijimos que $b \neq c$. Contradicción.

2.7. Problema 24.4

Si p es un primo y $p|a$ además que $p|(a^2 + b^2)$ implica que $p|b$

Demostración:

Sea $p|a$ por lo tanto $p|a^2$ y podemos decir que p divide a cualquier combinación lineal, por ejemplo $p|(-1)(a^2) + (1)(a^2 + b^2)$ por lo tanto $p|b^2$ pero como sabemos que p es un primo la unica forma de que divida a b. Por lo tanto $p|b$.

2.8. Problema 24.5

Si p es un primo y $p|a^n$ entonces $p|a$

Demostración:

Tenemos la factorización prima de a, el hecho de elevar a al cuadrado no crea o elimina factores primos, por lo tanto $p|a$ si y solo si $p|a^n$.

2.9. Problema 24.9

Si p es un primo y $p|(a^2 + b^2)$ y $p|(b^2 + c^2)$ entonces $p|(a^2 - c^2)$

Demostración:

Esto sale en un paso, pues p divide a cualquier combinación lineal de sus multiplos, es decir $p|(a^2 + b^2) - (b^2 + c^2)$, es decir $p|a^2 - c^2$

2.10. Problema 24.11

Si $(a, b) = 1$ entonces (a^2, ab, b^2)

Demostración:

Si $(a, b) = 1$ no comparten primos en común.

Recuerda:

Podemos también podemos decir que dados dos enteros escritos en su factorización prima tenemos que:

- $a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$
- $b = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$

Entonces podemos definir al máximo común divisor como:

$$GCD(a, b) = p_1^{min(e_1, f_1)} p_2^{min(e_2, f_2)} \dots p_k^{min(e_k, f_k)} \tag{1}$$

Por lo tanto a^2, b^2, ab ninguno creará primos en común que no existian en a, b. Por lo tanto (a^2, ab, b^2)

2.11. Problema 24.13

Contraejemplo: Si $b|(a^2 + 1)$ entonces $b|(a^4 + 1)$

Demostración:

Suponga $b = 5$ y $a = 2$, entonces $5|(4 + 1)$ pero no es cierto que $5|(16 + 1)$.

2.12. Problema 24.15

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

Demostración:

Podemos también podemos decir que dados dos enteros escritos en su factorización prima tenemos que:

- $a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$
- $b = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$
- $c = p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$

Por lo tanto:

$$\begin{aligned} GCD(a, b, c) &= p_1^{min(e_1, f_1, g_1)} \dots p_k^{min(e_k, f_k, g_k)} \\ &= p_1^{min(min(e_1, f_1), min(e_1, g_1))} \dots p_k^{min(min(e_k, f_k), min(e_k, g_k))} \\ &= GCD(GCD(a, b), GCD(b, c)) \end{aligned}$$

2.13. Problema 25

¿Para que enteros $\dfrac{n(n+1)}{2}|n!$

Demostración:

$\dfrac{n(n+1)}{2}|n!$ si y solo si $\dfrac{n!}{\frac{n(n+1)}{2}}$ pertenece a los enteros.

Por lo tanto $\dfrac{(n-1)!}{\frac{n+1}{2}}$ es decir si $\dfrac{2(n-1)!}{n+1}$.

Eso no pertenece a los enteros si n fuera par, pues $2(n-1)!$ son elementos pares y $n+1$ (al n ser par) es impar, por lo tanto es imposible encontrar factores para cancelarlo.

Si n fuera impar entonces el tenemos que la expansión de terminos de $2(n-1)!$ tiene un número par de factores, veamos el termino de enmedio más uno (por ejemplo el 3 en $(1)(2)(3)(4)$), aquel número en esa posción en la expansión $(n-1)!$ tendrá un valor de $\dfrac{n+1}{2}$ pero al multiplicarlo por dos tenemos justo un $n+1$ por lo tanto se cancela y dicho número será un entero.

$\dfrac{n(n+1)}{2}|n!$ si y solo si n es impar.

Quiza el último párrafo no quedará tan claro, así que unos ejemplos aquí:

- $\dfrac{2(5-1)!}{6} = \dfrac{2[(1)(2)(3)(4)]}{6} = \dfrac{(1)(2)(6)(4)}{6} = (1)(2)(4)$
- $\dfrac{2(9-1)!}{10} = \dfrac{2[(1)(2)(3)(4)(5)(6)(7)(8)]}{10} = \dfrac{(1)(2)(3)(4)(10)(6)(7)(8)}{10} = (1)(2)(3)(4)(6)(7)(8)$
- $\dfrac{2(7-1)!}{8} = \dfrac{2[(1)(2)(3)(4)(5)(6)]}{8} = \dfrac{(1)(2)(3)(8)(5)(6)}{8} = (1)(2)(3)(5)(6)$

2.14. Problema 28

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

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

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

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 la propiedad de arriba nos podría facilitar el cálculo.

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 $a < \sqrt{n}$.