Práctico 3: Números primos, Teorema fundamental de la Aritmética

Matías Iglesias

Diciembre 2018

1 Ejercicio 1

Ejercicio 1. Se consideran los siguientes números:

$$9000 \qquad 15^4 \cdot 42^3 \cdot 56^5 \qquad 10^n \cdot 11^{n+1}$$

a. Halllar la descomposición factorial de esos números.

b. ¿Cuántos divisores tienen?

c. ¿Es alguno de ellos un cuadrado perfecto?

a. $9000 = 9 \times 1000 = 3^2.10^3 = 2^3 3^2 5^3$.

b. Aplicando el segundo ítem del Corolario 1.7.6 de las Notas del Curso resulta que la cantidad de divisores se puede calcular como $|Div_+(9000)| = (2+1)(3+1)(3+1) = 48$

c. Aplicando el tercer ítem del Corolario 1.7.6 resulta que para que 9000 sea cuadrado perfecto se debe cumplir que todos los exponentes de la descomposición factorial han de ser pares; lo cual aquí no ocurre. Por lo tanto 9000 no es un cuadrado perfecto.

a. $15^4.42^3.56^5 = 3^4.5^4.2^3.3^3.7^3.2^{15}.7^5 = 2^{18}.3^7.5^4.7^8$.

b. Aplicando el segundo ítem del Corolario 1.7.6 de las Notas del Curso resulta que la cantidad de divisores se puede calcular como $|Div_+(15^4.42^3.56^5)| = (18+1)(7+1)(4+1)(8+1) = 6840$

c. Aplicando el tercer ítem del Corolario 1.7.6 resulta que para que $15^4.42^3.56^5$ sea cuadrado perfecto se debe cumplir que todos los exponentes de la descomposición factorial han de ser pares; lo cual aquí no ocurre. Por lo tanto $15^4.42^3.56^5$ no es un cuadrado perfecto.

a. $10^n.11^{n+1} = 2^n.5^n.11^{n+1}$.

b. Aplicando el segundo ítem del Corolario 1.7.6 de las Notas del Curso resulta que la cantidad de divisores se puede calcular como $|Div_+(10^n.11^{n+1})| = (n+1)(n+1)(n+2)$.

c. Aplicando el tercer ítem del Corolario 1.7.6 resulta que para que $15^4.42^3.56^5$ sea cuadrado perfecto se debe cumplir que todos los exponentes de la descomposición factorial han de ser pares; lo cual aquí no ocurre. Por lo tanto $15^4.42^3.56^5$ no es un cuadrado perfecto.

2 Ejercicio 2

Ejercicio 2. Hallar el menor número natural n tal que $6552 \cdot n$ sea un cuadrado perfecto.

Notemos que $6552n$ se puede escribir como $2^3.3^2.7.13n$. Ahora, utilizando el corolario ya utilzado en el ejercicio anterior resulta que $n = 2^1.7^1.13^1 = 182$ y por lo tanto 1192464 tiene como raíz cuadrada a 1092.

3 Ejercicio 3

Ejercicio 3. Decidir si existen enteros a y b que satisfagan

a. $a^2 = 8b^2$. **b**. $a^2 = 3b^3$. **c**. $7a^2 = 11b^2$.

a. Claramente el número dos debe aparecer en la descomposición factorial de a, pues si no apareciese no podría coincidir con $8b^2 = 2^3b^2$. Por lo tanto, $a = 2^{\alpha_0}p_1^{\alpha_1}...p_n^{\alpha_n}$ y $b = p_1'^{\alpha_1'}...p_n'^{\alpha_n'}$ donde p_i y p_i' son los primos correspondientes a la descomposición factorial de a y b respectivamente. Así pues, $2^{2\alpha_0}p_1^{2\alpha_1}...p_n^{2\alpha_n} = 2^3 p_1'^{2\alpha_1'}...p_n'^{2\alpha_n'}$. Ahora, si b no tiene al número dos en su descomposición factorial, entonces se deberá cumplir que $2\alpha_0 = 3$ y como $\alpha_0 \in \mathbb{N}$ esto no sería posible. Por tanto, b debería admitir al número dos en su descomposición factorial. Esto implicaría que $p_i' = 2$ para algún i. Pero entonces se debería cumplir que $2\alpha_0 = 2\alpha_i' + 3$ lo que implicaría que $\alpha_0 = \alpha_i' + 3/2$ pero claramente no puede ser. Esto prueba que no existen a y b tales que $a^2 = 8b^2$.

b. Sí existen, un ejemplo de esto es $a = 9$, $b = 3$.

c. Razonando de forma análoga a la realizada en la parte a. se concluye que no existen valores de a y b enteros tales que $7a^2 = 11b^2$.

4 Ejercicio 4

Ejercicio 4.

a. Sea $(p_n)_{n\in\mathbb{N}}$ la sucesión de los números primos, $p_1 = 2$, $p_2 = 3$, etc. Probar que para todo $n \in \mathbb{N}$ se tiene que $p_1p_2 \ldots p_n + 1 \geq p_{n+1}$. ¿Es cierto que $p_1p_2 \ldots p_n + 1$ es primo para todo $n \in \mathbb{N}$?

b. Hallar la factorización en producto de primos de 148500, 7114800, 7882875, 8!, 10! y 15!.

c. Si la factorización en producto de factores primos de $m \in \mathbb{N}$ es $m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, hallar la factorización en producto de números primos de m^2 y de m^3.

a. Sea $n = p_1p_2...p_n+1$. Al ser $n \geq 1$ por el Teorema Fundamental de la Aritmética, n se escribe como producto de primos. En particular, existe algún primo p_{n+1} que divide a n. Por lo tanto $p_{n+1} \leq n$ y esto termina la prueba. Se descarta el hecho de que p_n divide n claramente.

No es cierto que $p_1p_2...p_n + 1$ es primo para todo $n \in \mathbb{N}$ pues $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$.

b. $148500 = 2^2.3^3.5^3.11$, $7114800 = 2^4.3.5^2.7^2.11^2$, $8! = 2^7.3^2.5.7$, $10! = 2^8.3^4.5^2.7$ y $15! = 2^{11}.3^6.5^3.7^2.11.13$.

c. $m^2 = P_1^{2\alpha_1}P_2^{2\alpha_2}...P_k^{2\alpha_k}$ y $m^3 = P_1^{3\alpha_1}P_2^{3\alpha_2}...P_k^{3\alpha_k}$

5 Ejercicio 5

Ejercicio 5. Sea $A = \{4n + 1 : n = 0, 1, 2, \ldots\} = \{1, 5, 9, \ldots\}$. Un elemento $x \in A$, $x \neq 1$ se llama A-*primo* si los únicos divisores en A son 1 y x. Por ejemplo 9 es A-primo ya que 5 no divide a 9. Los elementos restantes de A, mayores que 1, se llaman A-*compuestos*.

- **a**. Probar que todo número A-compuesto se descompone en producto de factores A-primos.
- **b**. ¿La descomposición anterior es única? Sugerencia: Observe que el producto de dos primos de la forma $4k + 3$ es un A-primo.

a. Realicemos la prueba por inducción completa. Nuestro paso base es $n = 6$. Notemos que $25 = 5^2$. Supongamos por hipótesis inductiva que $1 < m < n$ se puede escribir como producto de $A - primos$ y demostremos la tésis inductiva que establece que n se puede escribir como producto de $A - primos$. Si n es $A - primo$ tenemos lo deseado de inmediato. En caso contrario existe $a \in A$ con $1 < a < n$. Por lo tanto, existe b con $1 < b < n$ tal que $n = a.b$. Dichos a y b están en las hipótesis inductiva. Por lo tanto se pueden escribir como producto de $A - primos$ y en consecuencia n también.

Sólo falta un detalle de la demostración que es considerar la posibilidad de que $b \notin A$. Por lo tanto b es de la forma $4k$, $4k+2$ y $4k+3$. Pero entonces, como $a \in A$ resulta que $a = 4l+1$ y notemos que los productos posibles son: $(4l+1)(4k+2) = 16kl+8l+4k+2 = 4(4kl+2l+k)+2$

liquidar

b. liquidar

6 Ejercicio 6

Ejercicio 6.

- **a**. Demostrar que $\sqrt{p}$ es irracional para cualquier primo p.
- **b**. Demostrar que $\log_{10} 2$ es irracional y que cuando p es primo $\log_{10} p$ es también irracional.

a. Supongamos por absurdo $\sqrt{2}$ es racional. Por lo tanto se puede escribir como $\frac{a}{b}$ con $a, b \in \mathbb{N}$. Ahora bien, resulta que $p.b^2 = a^2$ con $mcd(a, b) = 1$. Por lo tanto, utilizando el Teorema Fundamental de la Aritmética resulta que $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$ y $b = p_1'^{\beta_1} p_2'^{\beta_2} ... p_n'^{\beta_n}$. Pero como $p.b^2 = a^2$ y $mcd(a, b) = 1$ resulta que p debe aparecer en la descomposición factorial de a. Lo anterior implica que $2\alpha_i = 1$ para algún i. Pero esto es absurdo porque $\alpha_i \in \mathbb{N}$.

b. Seguir ideas de a.

7 Ejercicio 7

Ejercicio 7.

a. Determinar el menor cuadrado perfecto que es divisible entre $7!$.

b. Demostrar que $n \in \mathbb{N}$ es un cuadrado perfecto si y solamente si n tiene un número impar de divisores positivos.

c. Hallar el menor número natural n para el cual $1260 \times n$ es un cubo perfecto.

a. Primero notemos que $7! = 8!/8$ y utilizando el ejercicio 4.b resulta que $7! = 2^7.3^2.5.7/2^3 = 2^4.3^2.5.7$. Buscamos a^2 tal que $2^4.3^2.5.7|a^2$. Usando que $a = p_1^{\alpha_1}p_2^{\alpha_2}...p_n^{\alpha_n}$ resulta que $2^4.3^2.5.7|p_1^{2\alpha_1}p_2^{2\alpha_2}...p_n^{2\alpha_n}$. Por lo tanto se concluye que $\alpha_1 = 2, \alpha_2 = 2$ y por lo tanto $a = 2^2.3$.

b. Utilizando el Corolario 1.7.6 de las Notas del Curso tenemos que la cantidad de divisores posirivos de de n es $Div_+(n) = (e_1+1)(e_2+1)...(e_k+1)$ con $n = p_1^{e_1}p_2^{e_2}...p_n^{e_k}$. Ahora, n es un cuadrado perfecto si y sólo si $e_i = 2l$ para algún $l \in \mathbb{N}$. Por lo tanto, esto pasa si y sólo si la cantidad de divisores positivos se expresa como: $Div_+(n) = (2l_1+1)(2l_2+1)...(2l_k+1)$. Pero cada divisor tiene exponente $2l_i + 1$ y esto implica que n tiene un número impar de divisores.

c. $n \times 1260 = n \times 2^2.3^2.5.7$ y por ende $n = 2.3.5^2.7^2 = 7350$.

8 Ejercicio 8

Ejercicio 8. En un manicomio hay 2014 habitaciones numeradas con los números $1, 2, 3, \ldots, 2014$. En un principio están todas las puertas cerradas. Cuando pasa el primer paciente abre la puerta de cada habitación, luego pasa el segundo paciente y cierra las puertas $2, 4, 6, 8, \ldots$. Pasa el tercer paciente y cambia de estado las puertas $3, 6, 9, 12, \ldots$ (es decir, la cierra si estaba abierta y la abre si estaba cerrada) y así hasta que pasa el paciente 2014 que cambia de estado la puerta 2014. ¿Cuántas puertas abiertas quedan luego de pasar los 2014 pacientes?

La solución supuestamente es la parte entera de $\sqrt{2}014$ que es 44. Sale utilizando divisores positivos y ejercicio 7 supuestamente...
liquidar

9 Ejercicio 9

Ejercicio 9. Hallar los números naturales menores o iguales a 1000 que tienen exactamente 3 divisores positivos distintos.

Utilizando el Corolario 1.7.6 de las Notas del Curso tenemos que encontrar los números $a \in \mathbb{N}$ tales que $0 \leq a \leq 1000$ con $Div_+(a) = (1+e_1)(1+e_2)(1+e_3) = 3$ donde $a = p_1^{e_1}p_2^{e_2}p_3^{e_3}$. Observando la ecuación de divisores vemos que $e_i \neq 1\ \forall i$ pues quedaría que un número par es igual a un número impar. Además se ve que e_i no puede ser igual o superior 3. Por lo tanto sólo quedan los casos en que $e_i = 0$ y $e_i = 2$. Supongamos que $e_i = 0$ para algún i, entonces la ecuación de divisores queda $(1+e_j)(1+e_k) = 3$ con $j \neq k$. Aquí vemos que e_j no puede ser mayor o igual que 3 y no puede ser 1, por ende quedan las opciones 0 y 2. Pero si es 2 el restante ha de ser 0 y viceversa. Por lo tanto, por la simetría del problema vemos que la única opción válida es que $a = p_1^2$ con p_1 primo y $0 \leq a \leq 1000$. Pero entonces $0 \leq p_1 \leq 31$. Por lo tanto, $p_1 \in \{2, 3, 5, 7, 11, 13, 17, 23, 29, 31\}$ y por ende $a \in \{2^2, 3^2, 5^2, 7^2, 11^2, 13^2, 17^2, 23^2, 29^2, 31^2\}$ resultando en que $a \in \{4, 9, 25, 49, 121, 169, 289, 529, 841, 961\}$

10 Ejercicio 10

Ejercicio 10. Hallar los números naturales a y b que cumplen que el resto de dividir a entre b es 5 y que $\mathrm{mcm}(a, b) = 12 \times \mathrm{mcd}(a, b)$.

Tenemos que $a = bq + 5$ con $q \in \mathbb{N}$ y definiendo $d = mcd(a, b)$ resulta que $ab = 12d^2$. Por otro lado, $d|a$ y $d|b$ por lo tanto $d|a - bq = 5$ conforme con la propiedad 10 de la lista de Propiedades 1.1.5 de las Notas del Curso. Por lo tanto $d = 5$ o $d = 1$. Analicemos primeramente el caso en que $d = 5$. Entonces resulta que $ab = 2^2.3.5^2$. Ahora bien, cómo $d = 5$ es el máximo común divisor de a y b resulta que debe estar en la descomposición factorial de ellos, por lo tanto $a = 2^{e_1}3^{e_2}5$ y $a = 2^{e'_1}3^{e'_2}5$ con las condiciones $e_1 + e'_1 = 2$ y $e_2 + e'_2 = 1$. Por lo tanto, hay 6 casos posibles que son los que resumimos en la siguiente tabla

e_1	e'_1	e_2	e'_2	a	b
2	0	1	0	60	5
2	0	0	1	20	15
1	1	1	0	30	10
1	1	0	1	10	30
0	2	1	0	15	20
0	2	0	1	5	60

Pero de los casos anteriores sólo sirven aquellos en los que el resto de dividir a entre b da 5 y por lo tanto los caso serían: $a = 20, b = 15$ $(q = 1)$ y $a = 5, b = 60$ $(q = 0)$.

El caso en que $d = 1$ implica que $a.b = 2^2.3$. Claramente a no puede ser 12 pues esto dejaría que $b = 1$ y por ende no podría cumplirse la primera condición del ejercicio. Si $a = 6$ entonces necesariamente $b = 2$ pero tampoco se cumpliría la primera condición del ejercicio. Los restantes valores posibles para a son 1,2,3,4 y se ve también rápidamente que no cumplen las hipótesis del ejercicio.

11 Ejercicio 11

Ejercicio 11. ¿Cuántas parejas de números naturales coprimos (a, b) verifican que $a + b = 1000$?

Buscamos hallar $mcd(a, b) = mcd(a, 1000 - a) = 1$. Recordando la Proposición 1.2.6 de las Notas del Curso tenemos que $mcd(a, b) = mcd(a, 1000 - a) = mcd(a, 1000) = 1$. Por lo tanto los divisores de a no pueden ser los divisores de 1000. Como $1000 = 2^3.5^3$ resulta que a no puede ser múltiplo de dos ni de cinco. Además $a \in [0, 1000]$ por lo tanto a tiene tres dígitos. Imponiendo que el último dígito de a no puede ser múltiplo de dos ni de cinco se tiene que dicho dígito podrá ser: 1,3,7 y 9. No hay restricciones para los dos primeros dígitos, por lo tanto estos pueden variar entre 0 y 9. Entonces debemos sumar todos los casos posibles: $10 \times 10 \times 4 = 400$.

12 Ejercicio 12

Ejercicio 12. Hallar los números naturales a y b sabiendo que $\mathrm{mcd}(a, b) = 18$, que a tiene 21 divisores y que b tiene 10.

Aplicando conocimientos ya vistos en este práctico resulta que la cantidad de divisores de a se puede expresar como $(e_1 + 1)(e_2 + 1) = 3.7$ y por lo tanto $e_1 = 2$ y $e_2 = 6$ ó $e_1 = 6$ y $e_2 = 2$. Idéntico razonamiento vale para b y se llega a que $e'_1 = 1$ y $e'_2 = 4$ ó $e'_1 = 4$ y $e'_2 = 1$. Por otro lado, como $mcd(a, b) = 18 = 2.3^2$ resulta que $3^2.2$ debe aparecer en la descomposición factorial de a y b. De todo lo anterior se tiene que $a = p_1^{\alpha_1} p_2^{\alpha_2}$ y $b = q_1^{\beta_1} q_2^{\beta_2}$. Juntando todo lo anterior resulta que $a = 2^6.3^2 = 576$ y $b = 2.3^4 = 162$.

13 Ejercicio 13

Ejercicio 13.

a. Sean a y b naturales primos entre sí. Probar las siguientes afirmaciones.

- **i)** a^2 y b^2 son primos entre sí.
- **ii)** $a + b$ y ab son primos entre sí.

b. Determinar las parejas de números naturales (a, b) que verifican $5 \times (a + b)^2 = 147 \times \mathrm{mcm}(a, b)$.

a. i) Sea $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$ y $b = p_1^{\beta_1} p_2^{\beta_2} ... p_n^{\beta_n}$. Por lo tanto $a^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} ... p_n^{2\alpha_n}$ y $b^2 = p_1^{2\beta_1} p_2^{2\beta_2} ... p_n^{2\beta_n}$. Entonces $mcd(a^2, b^2) = \prod_{i=1}^n p_i^{\min\{2\alpha_i, 2\beta_i\}} = \prod_{i=1}^n p_i^{2\min\{\alpha_i, \beta_i\}} = (\prod_{i=1}^n p_i^{\min\{\alpha_i, \beta_i\}})^2 = mcd(a, b)^2 = 1$.

ii) Sea $d = mcd(a + b, ab)$. Por definición $d|a + b$ y también divide a cualquier combinación lineal de ellos (propiedad 10 de Propiedadesd 1.1.5 de las Notas del Curso, tomando $x = y = b$). Por lo tanto $d|ab + b^2$. Por lo tanto $d|b^2$ ya que $d|ab$ por hipótesis. Idéntico razonamiento prueba que $d|a^2$. Por lo tanto $d|a^2 + b^2$.Entonces $d|mcd(a^2, b^2) = 1$. Por lo tanto $d|1$ y se tiene que $mcd(a + b, ab) = 1$.

b. Definimos $d = mcd(a, b)$, $a = a{*}d$ y $b = b{*}d$ con $mcd(a*, b*) = 1$. Por lo tanto $5d(a{*}+b{*})^2 = 3.7^2.a * .b*$. Por lo probado en las partes anteriores resulta que $mcd(a * +b*, a * b*) = 1$. Entonces $a{*}+b{*} \mid 7$. Por lo tanto $a{*}+b{*} = 1$ ó $a{*}+b{*} = 7$. Además $5d = 3a{*}b{*}$. Analicemos primeramente el caso en que $a * +b* = 1$ se descarta rápidamente pues $mcm(1, 0) = 0$ ya que $mcd(1, 0) = 1$ y $mcd(1, 0).mcm(1, 0) = 1 \times 0 = 0$. Por lo tanto queda el caso que $a * +b* = 7$.

$a*$	$b*$
1	6
2	5
3	4
4	3
5	2
6	1

Inspeccionando la tabla anterior se ve que los únicos valores que dan $d \in \mathbb{N}$ son $a* = 2, b* = 5$ y $a* = 5, b* = 2$. Para estos valores se tiene que $d = 6$ y por lo tanto $a = 12, b = 30$ y $a = 30, b = 12$.

14 Ejercicio 14

Ejercicio 14.

a. Probar que si $p > 2$ es primo, entonces es de la forma $4k \pm 1$, para algún $k \in \mathbb{Z}$.

b. Probar que si $p > 3$ es primo, entonces es de la forma $6k \pm 1$, para algún $k \in \mathbb{Z}$.

c. Probar que existen infinitos primos de la forma $4k - 1$.
Sugerencia: imitar la prueba de Euclides sobre la infinitud de primos.

a. Todos los números enteros se pueden expresar como $4k$, $4k \pm 1$, $4k \pm 2$ y $4k \pm 3$ con $k \in \mathbb{Z}$. Ahora, primero notemos que $4k \pm 3 = 4(k \pm 1) \pm 1 = 4k' \pm 1$ para algún $k' \in \mathbb{Z}$. Por lo tanto, debemos probar que si $p > 2$ primo no es de la forma $4k \pm 1$, $4k \pm 2$. Claramente esto es cierto pues la cantidad de divisores positivos de $4k \pm 1$ y $4k \pm 2$ es mayor a 2, ya que en el primer caso tanto $1, 2, k, 2k$ lo dividen y en el segundo caso $1, 2, 2k \pm 1$ lo dividen.

b. Siguiendo las ideas de la parte anterior vemos que todos los números se escriben como $6k, 6k \pm 1, 6k \pm 2, 6k \pm 3, 6k \pm 4, 6k \pm 5$ para algún $k \in \mathbb{Z}$. Ahora, al igual que en la parte anterior se descartan rápidamente las posibilidades $6k, 6k \pm 2, 6k \pm 4$. El caso $6k \pm 3 = 3(2k \pm 1)$ también se descarta. Analicemos qué ocurre con el caso $6k \pm 5 = 6(k \pm 1) \pm 1 = 6k' \pm 1$ para algún k'. Por lo tanto, hemos probado lo que se quería.

c. Supongamos por absurdo que los primos de la forma $4k - 1$ son finitos. Definimos $C = \{p_1, p2, ..., p_k\}$ el conjunto de todos los primos. Consideremos un natural $n = 4(p_1 p_2 ... p_k) - 1$. Por el Teorema Fundamental de la Aritmética existe la factorización del número n (≥ 2) en números primos. Por lo tanto existe algún primo $p_i \in C$ que es divisor de n. Entonces tenemos que $p_i | n$ y $p_i | 4(p_1 p_2 ... p_k)$ y por la propiedad 10 (tan comentada en este práctico) $p_i | 4(p_1 p_2 ... p_k) - n = 1$. Ahora bien, el único divisor natural de 1 es 1 y como p_i es primo esto conduce a un absurdo ya que que $p_i \nmid 1$. Este absurdo fue suponer que la cantidad de primos de la forma $4k - 1$ es finita y por lo tanto existen infinitos primos de esa forma.

15 Ejercicio 15

Ejercicio 15. Sea $n = p^\alpha q^\beta$ la descomposición en producto de factores primos de un natural n. Si n no es un cuadrado perfecto calcular el producto de los divisores de n.

Se nos pide calcular $p^0 p^1 ... p^\alpha q^0 q^1 ... p^\beta = p^{\sum_{i=0}^{i=\alpha}} q^{\sum_{i=0}^{i=\beta}} = p^{\alpha(\alpha+1)/2} q^{\beta(\beta+1)/2}$.

16 Ejercicio 16

Ejercicio 16.

a. Diremos que un par de enteros coprimos (x_1, x_2) es reducible si existe $n_1 \in \mathbb{Z}$ tal que $x_1 + n_1 x_2 = 1$.

i) Dar un ejemplo de un par de coprimos reducible.

ii) Dar un ejemplo de un par de coprimos no reducible (justificar).

b. Diremos que una terna de enteros (x_1, x_2, x_3) son coprimos si existen $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}$ tal que $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 = 1$.

i) Dar un ejemplo de una terna de coprimos tal que cada par de enteros (x_i, x_j), con $1 \leq i, j \leq 3$, no sean coprimos.

ii) Demostrar que (x_1, x_2, x_3) son coprimos si y solamente si no existe un primo p que divida a x_i para $i = 1, 2, 3$.

a. i) (7,3) pues $7 + (-2) \times 3 = 1$.

ii) (3,7) pues $3 + 7n = 1$ implicaría que 7 divide a 2 y esto no es verdad.

b. i) (6,10,15) pues $1 \times 6 + 1 \times 10 + (-1) \times 15 = 1$ y $mcd(6, 10) = 2$; $mcd(10, 15) = 5$; y $mcd(6, 15) = 3$.

ii) Directo: si (x_1, x_2, x_3) son coprimos, existen, por definición $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}$ tal que $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 = 1$. Si $m \in \mathbb{Z}$ divide a x_1, x_2, x_3, entonces m divide a $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 = 1$. Luego $m = \pm 1$. Esto prueba el directo.

Recíproco: sea $d = mcd(x_1, x_2)$. Entonces, por el Lema de Bezout, existen $\beta_1, \beta_2 \in \mathbb{Z}$ tales que $d = \beta_1 \times x_1 + \beta_2 \times x_2$. Por hipótesis $mcd(d, x_3) = 1$. Entonces existen $\gamma, \alpha_3 \in \mathbb{Z}$ tal que $\gamma \times d + \alpha_3 \times x_3 = 1$. Sustituyendo obtenemos: $\gamma \times (\beta_1 \times x_1 + \beta_2 \times x_2) + \alpha_3 \times x_3 = 1$. Luego, definiendo $\alpha_1 = \gamma \times \beta_1$ y $\alpha_2 = \gamma \times \beta_2$ se obtiene el resultado.

17 Ejercicio 17

Ejercicio 17. Sea p primo y supongamos que $p^2 | ab$. Demostrar que si $\mathrm{mcd}(a, b) = 1$, entonces $p^2 | a$ or $p^2 | b$.

Claramente p^2 no es primo pues tiene a $1, p, p^2$ como divisores. Ahora bien, p^2 tiene por el Teorema Fundamental de la Aritmética descomposición factorial en números primos. Pero como $p^2 \mid ab$ resulta que al ser $mcd(a, b) = 1$ necesariamente los divisores de a no son divisores de b. Por lo tanto, los divisores de p^2 deben dividir a a o b.

Nerd

18 Ejercicio 18

Ejercicio 18.

a. Demostrar que $\operatorname{mcd}(a^2, b^2) = \operatorname{mcd}(a, b)^2$.

b. Demostrar que si $n \geq 1$, entonces $\operatorname{mcd}(a^n, b^n) = \operatorname{mcd}(a, b)^n$.

a. Imitar demostración del ejercicio 13.a

b. Realizaremos la prueba por inducción completa. Notemos que nuestro paso base para $n = 2$ es válido por la parte anterior. Ahora sumamos que $mcd(a^n, b^n) = mcd(a, b)^n$ por hipótesis inductiva y demostremos nuestra tésis inductiva. Pero notemos que $mcd(a, b)^{n+1} = mcd(a, b)^n mcd(a, b) = mcd(a^n, b^n) mcd(a, b)$. Ahora sólo resta escribir la descomposición en factores primos para a y b y se tiene rápidamente la tésis.

19 Ejercicio 19

Ejercicio 19.

a. Probar que si p es primo, entonces $p | \binom{p}{i}$ para todo $0 < i < p$ (donde $\binom{p}{i}$ son las combinaciones de p en i).

b. ¿Es cierto lo anterior si p no es primo?