Álgebra I

Darvid

November 12, 2021

1 Capítulo 0. Propiedades de los números enteros

P1. $b|b$, para cada $b\in\mathbb{Z}$.

P2. $b|0$, para cada $b\in\mathbb{Z}$.

P3. $1|a$ y $-1|a$, para cada $a\in\mathbb{Z}$.

P4. $0|a \iff a=0$.

P5. Si $b|1$, entonces $b=\pm1$.

P6. Si $b|a$ y $a|b$, entonces $a=\pm b$.

P7. Si $b|a$ y $a|c$, entonces $b|c$.

P8. Si $b|a$ y $b|c$, entonces $b|a+c$ y $b|a-c$.

P9. Si $b|a$, entonces $b|ac$ $\forall c\in\mathbb{Z}$.

P10. Si $b|a$ y $b|c$, entonces $b|as+ct$ $\forall s,t\in\mathbb{Z}$.

P11. $b|a \iff b|-a \iff -b|a \iff -b|-a$.

P12. $b|a \iff b\Big||a| \iff |b|\Big|a \iff |b|\Big||a|$.

P13. Si $b|a+c$ y $b|a$, entonces $b|c$.

Demostración:

P1. Notemos que $b=b\cdot1$, $\forall b\in\mathbb{Z}$. Entonces $b|b$, para cada $b\in\mathbb{Z}$.

P2. Notemos que $0=b\cdot0$, $\forall b\in\mathbb{Z}$. Entonces $b|0$, para cada $b\in\mathbb{Z}$.

P3. Notemos que $a=1\cdot a$ y $a=(-1)\cdot(-a)$, $\forall a\in\mathbb{Z}$. Entonces $1|a$ y $-1|a$, para cada $a\in\mathbb{Z}$.

P4.
- **i)** Si $0|a$, entonces $\exists q\in\mathbb{Z}$ tal que $a=0\cdot q$, por lo que $a=0$.
- **ii)** Si $a=0$, se verifica que $\exists q\in\mathbb{Z}$ tal que $a=0\cdot q$, por lo que $0|a$.

P5. Si $b|1$, entonces $\exists q\in\mathbb{Z}$ tal que $1=bq$. Como $1>0$ se verifica que $|bq|=bq$. Además $|bq|=|b||q|$, por lo que $1=|b||q|$. Por definición $|b|\geq0$ y $|q|\geq0$, pero $b\neq0$ y $q\neq0$, entonces $|b|>0$ y $|q|>0$. Luego, como $|b|,|q|\in\mathbb{N}$ sigue que $|b|\geq1$ y $|q|\geq1$, pero $|b|>1$ contradice nuestra hipótesis. Por tanto, $b=\pm1$.

P6. Si $b|a$ y $a|b$, entonces $\exists q_1,q_2\in\mathbb{Z}$ tales que $a=bq_1$ y $b=aq_2$. De este modo, $a=a(q_1q_2)$. Suponiendo que $a\neq 0$, tenemos que $1=q_1q_2$, lo cual implica que $q_1|1$ y por (A5), $q_1=\pm 1$. Por tanto, $a=\pm b$.

P7. Si $b|a$ y $b|c$, entonces $\exists q_1,q_2\in\mathbb{Z}$ tales que $a=bq_1$ y $c=aq_2$. De este modo, $c=b(q_1q_2)$, es decir, $b|c$.

P8. Si $b|a$ y $b|c$, entonces $\exists q_1,q_2\in\mathbb{Z}$ tales que $a=bq_1$ y $c=bq_2$. De este modo, $a+c=bq_1+bq_2$, es decir $a+c=b(q_1+q_2)$ lo que implica que $b|a+c$. Similarmente, $a-c=bq_1-bq_2$, es decir, $a-c=b(q_1-q_2)$ lo que implica que $b|a-c$.

P9. Si $b|a$, entonces $\exists q\in\mathbb{Z}$ tal que $a=bq$. Sea $c\in\mathbb{Z}$ arbitrario pero fijo. Notemos que $ac=bqc$, lo que implica que $b|ac$, $\forall c\in\mathbb{Z}$.

P10. Si $b|a$ y $b|c$, entonces $\exists q_1,q_2\in\mathbb{Z}$ tales que $a=bq_1$ y $c=bq_2$. Sean $s,t\in\mathbb{Z}$ arbitrarios pero fijos, entonces $as=bq_1s$ y $ct=bq_2t$. De este modo, $as+ct=bq_1s+bq_2t$, es decir $as+ct=b(q_1s+q_2t)$, lo cual implica que $b|as+ct$.

P11.

i) Si $b|a$, entonces $\exists q\in\mathbb{Z}$ tal que $a=bq$. Notemos que $-a=-bq$, es decir $-a=b(-q)$ lo que implica que $b|-a$.

ii) Si $b|-a$, entonces $\exists q\in\mathbb{Z}$ tal que $-a=bq$. Notemos que $a=-bq$, lo que implica que $-b|a$.

iii) Si $-b|a$, entonces $\exists q\in\mathbb{Z}$ tal que $a=-bq$. Notemos que $-a=-(-bq)$, es decir, $-a=-b(-q)$, lo que implica que $-b|-a$.

iv) Si $-b|-a$, entonces $\exists q\in\mathbb{Z}$ tal que $-a=-bq$. Notemos que $a=bq$, lo que implica que $b|a$.

P12.

i) Si $b|a$, entonces $\exists q\in\mathbb{Z}$ tal que $a=bq$.

a) Si $a\geq 0$, entonces $|a|=a$, por lo que $a=bq$, lo cual implica que $b\,\big|\,|a|$.

b) Si $a\leq 0$, entonces $|a|=-a$, por lo que $-a=b(-q)$, lo cual implica que $b\,\big|\,|a|$.

ii) Si $b\,\big|\,|a|$, entonces $\exists q\in\mathbb{Z}$ tal que $|a|=bq$.

a) Si $a\geq 0$ y $b\geq 0$, entonces $|a|=a$ y $|b|=b$, por lo que $a=|b|q$, lo cual implica que $|b|\,\big|\,a$.

b) Si $a\geq 0$ y $b<0$, entonces $|a|=a$ y $|b|=-b$, por lo que $-|a|=-bq$, es decir, $-a=|b|q$. Notemos que $a=|b|(-q)$, lo cual implica que $|b|\,\big|\,a$.

c) Si $a<0$ y $b\geq 0$, entonces $|a|=-a$ y $|b|=b$, por lo que $-|a|=b(-q)$, es decir, $a=|b|(-q)$, lo cual implica que $|b|\,\big|\,a$.

d) Si $a<0$ y $b<0$, entonces $|a|=-a$ y $|b|=-b$, por lo que $-|a|=-bq$, es decir, $a=|b|q$, lo cual implica que $|b|\,\big|\,a$.

iii) Si $|b|\,\big|\,a$, entonces $\exists q\in\mathbb{Z}$ tal que $a=|b|q$

a) Si $a\geq 0$, entonces $|a|=a$, por lo que $|a|=|b|q$, lo cual implica que $|b|\,\big|\,|a|$.

b) Si $a<0$, entonces $|a|=-a$, por lo que $-a=-|b|q$, es decir, $|a|=|b|(-q)$, lo cual implica que $|b|\,\big|\,|a|$.

iv) Si $|b|\,\big|\,|a|$, entonces $\exists q\in\mathbb{Z}$ tal que $|a|=|b|q$.

a) Si $a\geq 0$ y $b\geq 0$, entonces $|a|=a$ y $|b|=b$, por lo que $a=bq$, lo cual implica que $b|a$.

b) Si $a\geq 0$ y $b<0$, entonces $|a|=a$ y $|b|=-b$, por lo que $a=-bq$, es decir, $a=b(-q)$, lo cual implica que $b|a$.

c) Si $a<0$ y $b\geq 0$, entonces $|a|=-a$ y $|b|=b$, por lo que $-a=bq$, es decir $a=b(-q)$, lo cual implica que $b|a$.

d) Si $a<0$ y $b<0$, entonces $|a|=-a$ y $|b|=-b$, por lo que $-a=-bq$, es decir, $a=bq$, lo cual implica que $b|a$.

P13. Si $b|a+c$ y $b|a$, entonces $\exists q_1,q_2 \in \mathbb{Z}$ tales que $a+c=bq_1$ y $a=bq_2$. Luego, $(bq_2)+c=bq_1$, es decir, $c=b(q_1-q_2)$, lo que implica que $b|c$.

Definición. Sean $a,b,c\in\mathbb{Z}$. Decimos que c es combinación lineal de a y b si existen $x,y\in\mathbb{Z}$ tales que $c=ax+by$.

2 Ejercicios

1.1 Pruebe que 29 es combinación lineal de 5 y 7.

1.2 Escriba a 50 en dos formas diferentes como combinación lineal de 5 y 2.

1.3 Si $d|a$, $d|b$ y $d\nmid c$, pruebe que c no es combinación lineal de a y b.

1.4 Pruebe que 64 no es combinación lineal de 10 y 25.

1.5 Encuentre un entero m que no sea combinación lineal de 28 y 49.

1.6 Si m divide a cualquier combinación lineal de a y b, pruebe que $m|a$ y $m|b$.

1.7 Decida si la ecuación $153=34x+51y$ tiene soluciones enteras x y y.

1.8 Si c es impar, pruebe que la ecuación $c=14x+72y$ no tiene soluciones enteras x y y.

2. Si $b|m$ para todo $m\in\mathbb{Z}$, pruebe que $b=\pm1$.

3. Si $b|a_1,b|a_2,...,b|a_n$, pruebe que $b|a_1+a_2+\cdots+a_n$.

4. Pruebe que

4.1 $8|(2n-1)^2-1$, para cada $n\in\mathbb{N}$.
4.2 $6|n^3-n$, para cada $n\in\mathbb{N}$.
4.3 $9|n^3+(n+1)^3+(n+2)^3$, para cada $n\in\mathbb{N}$.
4.4 $133|11^{n+2}+12^{2n+1}$, para cada $n\in\mathbb{N}$.
4.5 Si a,b,c son dígitos, entonces 143 divide al número (cifrado) $abcabc$.

5. Si $a,b\in\mathbb{Z}$, pruebe que $a-b|a^n-b^n$, para cada $n\in\mathbb{N}$.

6. Sean $a,b\in\mathbb{Z}$, con $b\neq0$. Pruebe que $b|a$, si y solo si, el residuo de dividir a por b, es $r=0$.

7. Aplicando el algoritmo de división , encuentre q y r para escribir $a=bq+r$ en los siguientes casos:

7.10 $a=m^3+3m^2+3m+2$ y $b=m+1$ $(m>0)$.

8. Pruebe que $(a,b)=(|a|,|b|)$.

9. Aplicando el algoritmo de Euclides y el ejercicio anterior, encuentre el mcd de:

9.5 $a=764$ y $b=-866$.

10. Si $(a,b)=1$, pruebe que la ecuación $c=ax+by$ tiene soluciones enteras x y y, para cada $c\in\mathbb{Z}$.

11. Sean $a,b,c\in\mathbb{Z}$. Si $d=(a,b)$, pruebe que la ecuación $c=ax+by$ tiene soluciones enteras, si y solo si, $d|c$.

12. Si $d>0$ es tal que $d|a$, $d|b$ y $d=as+bt$, pruebe que $d=(a,b)$.

13. Si $d=(a,b)$ y $d=as+bt$, pruebe que $(s,t)=1$. [¿Son únicos s y t?].

14. Si $d=(a,b)$, $a=bq_1$ y $b=dq_2$, pruebe que $(q_1,q_2)=1$.

15. Si $c|a$ y $(a,b)=1$, pruebe que $(b,c)=1$.

16. Si $a|c$, $b|c$ y $d=(a,b)$, pruebe que $ab|cd$.

17. Si $(a,b)=1$ y $c\neq 0$, pruebe que $(a,bc)=(a,c)$.

18. Si $k>0$, pruebe que $(ak,bk)=k(a,b)$.

19. Si $k\neq 0$, pruebe que $(ak,bk)=|k|(a,b)$.

20. Si $(a,b)=1$, pruebe que $(a+b,a-b)=1$ ó 2.

21. Si $(a,b)=1$, pruebe que $(a^m,b^n)=1$ para todo $n,m\in\mathbb{N}$.

22. Si $(a,b)=k$, pruebe que $(a^n,b^n)=k^n$ para todo $n\in\mathbb{N}$.

23. Sean $m,n,k\in\mathbb{N}$. Si $mn=k^2$ y $(m,n)=1$, pruebe que $m=a^2$ y $n=b^2$ para algunos $a,b\in\mathbb{N}$.

24. Si $(a,c)=1$ y $(b,c)=1$, pruebe que $(ab,c)=1$.

25. Si $b^2|a^2$, prube que $b|a$.

26. Si $b^n|a^n$, pruebe que $b|a$.

27. Si $a\in\mathbb{N}$ y $a\neq k^2$ para todo $k\in\mathbb{N}$, pruebe que $\sqrt{a}\notin\mathbb{Q}$.

28. Si $a\in\mathbb{N}$ y $a\neq k^n$ para todo $k\in\mathbb{N}$, pruebe que $\sqrt[n]{a}\notin\mathbb{Q}$.

29. Si $a_1,a_2,...,a_n$ son dígitos, pruebe que $9|a_1a_2...a_n$, si y solo si, $9|a_1+a_2+...a_n$ ($a_1a_2...a_n$ es un número cifrado). Sugerencia: Pruebe y use que $9|10^n-1$, para cada $n\in\mathbb{N}$.

30.1 Si $d=(a_0,a_1,...,a_n)$, pruebe que d es único.

31. Sean $a,b,c\in\mathbb{Z}$, no todos cero. Pruebe que $(a,b,c)=\big((a,b),c\big)$.

32. Sean $a_0,a_1,...,a_n\in\mathbb{Z}$, no todos cero. Pruebe que $(a_1,a_2,...,a_n)=\big(|a_1|,|a_2|,...,|a_n|\big)$.

33. Sean $a,b\in\mathbb{Z}$ con $a\neq 0$ y $b\neq 0$. Decimos que $m\in\mathbb{Z}$, $m>0$ es mínimo común múltiplo (mcm) de a y b, y escribimos $m=[a,b]$ ó $m=$ mcm $\{a,b\}$, si:

- **i)** $a|m$ y $b|m$.
- **ii)** Si $a|s$ y $b|s$ para algún $s\in\mathbb{Z}$, entonces $m|s$.

33.1 Si $m=[a,b]$, pruebe que m es único.

33.2 Dados $a,b\in\mathbb{Z}-\{0\}$, pruebe que existe $m=[a,b]$.

33.3 Pruebe que $[a,b]=\big[|a|,|b|\big]$.

33.4 Si $a>0$ y $b>0$ pruebe que $[a,b]=\frac{a\cdot b}{(a,b)}$.

33.5 Si $k>0$, pruebe que $[ak,bk]=k[a,b]$.

37. Si p es primo y $p|a_1\cdot a_2\cdot\dots\cdot a_n$, pruebe que $p|a_i$ para algún $i=1,2,...,n$.

38. Si $a \in \mathbb{Z}$ y $a < -1$, pruebe que existen primos $p_1, p_2, \ldots, p_n$ tales que $a = -p_1 \cdot p_2 \cdot \cdots \cdot p_n$.

40. Sea $n \in \mathbb{N}$. Si $2^n - 1$ es primo, pruebe que n es primo.

43. Si p es un número primo y $n \in \mathbb{N}$, pruebe que la suma de los divisores positivos de p^{n-1} es $\frac{p^n - 1}{p-1}$.

44. Pruebe que el conjunto de números primos no es finito.

Demostración:

1.1 Notemos que $29 = (5)(3) + (7)(2)$, es decir, existen $s, t \in \mathbb{Z}$ tales que $29 = 5s + 7t$, por lo que 29 es una combinación lineal de 5 y 7.

1.2 $50 = (5)(10) + (2)(0)$ y $50 = (5)(2) + (2)(20)$.

1.3 Supongamos que c es combinación lineal de a y b, entonces $\exists s, t \in \mathbb{Z}$ tales que $c = as + bt$. Si $d|a$ y $d|b$, entonces $\exists q_1, q_2 \in \mathbb{Z}$ tales que $a = dq_1$ y $b = dq_2$. Luego, $as = dq_1 s$ y $bt = dq_2 t$. De este modo, $as + bt = dq_1 s + dq_2 t$, es decir, $as + bt = d(q_1 s + q_2 t)$, lo cual implica que $d|c$, pero esto contradice nuestra suposición. Por tanto, c es combinación lineal de a y b.

1.4 Supongamos que 64 es combinación lineal de 10 y 25, entonces $\exists s, t \in \mathbb{Z}$ tales que $64 = 10s + 25t$. Notemos que $64 = 5(2s + 5t)$, lo cual implica que $5|64$, pero 64 no satisface la divisibilidad por 5. Por tanto, 64 no es combinación lineal de 10 y 25.

1.5 $m = 1$.

1.6 Si $m|as + bt \ \forall s, t \in \mathbb{Z}$, entonces elegimos $s = 1$ y $t = 0$, por lo que $m|a$. Luego, elegimos $s = 0$ y $t = 1$, por lo que $m|b$.

1.7 Dada la ecuación $153 = 34x + 51y$, notemos que $153 = (17)(9)$ y $34x + 51y = 17(2x + 3y)$, entonces $9 = 2x + 3y$, por lo que la ecuación tiene soluciones enteras $x = 3$ y $y = 1$.

1.8 Dada la ecuación $c = 14x + 72y$, tenemos que $c = 2(7x + 36y)$, lo cual implica que $2|c$, pero esto contradice la hipótesis de que c es impar.

2. Si $b|m \ \forall m \in \mathbb{Z}$, elegimos $m = 1$, por lo que $b|1$ y, por **(P5)**, sigue que $b = \pm 1$.

3. Procedamos por inducción sobre el número de elementos.

- **i)** Si $b|a_1$ y $b|a_2$, por **(P8)** se verifica que $b|a_1 + a_2$.
- **ii)** Supongamos que si $b|a_1, b|a_2, \ldots, b|a_k$, entonces $b|a_1 + a_2 + \ldots + a_k$.
- **iii)** Si $b|a_1, b|a_2, \ldots, b|a_k, b|a_{k+1}$, por hipótesis de inducción tenemos que $b|a_1 + a_2 + \ldots + a_k$, y dado que $b|a_{k+1}$ por **(P8)** se verifica que $b|a_1 + a_2 + \ldots + a_k + a_{k+1}$.

Por tanto, si $b|a_1, b|a_2, \ldots, b|a_n$, entonces $b|a_1 + a_2 + \cdots + a_n$, $\forall n \in \mathbb{N}$ con $n \geq 2$.

4.1 Procederemos por inducción en n.

- **i)** Verificamos que se cumple para $n = 1$.
  En efecto, $8|(2 \cdot 1 - 1)^2 - 1$, es decir, $8|0$, lo cual se verifica por **(P2)**.

ii) Supongamos que se cumple para $n=k$, es decir, supongamos que $8|(2k-1)^2-1$
Lo que implica que $\exists q\in\mathbb{Z}$ tal que

$$\begin{aligned}8q&=(2k-1)^2-1\\&=(4k^2-4k+1)-1\\&=4k^2-4k\end{aligned}$$

iii) Luego, si $n=k+1$, tenemos que

$$\begin{aligned}4(k+1)^2-4(k+1)&=4(k^2+2k+1)-4k-4\\&=4k^2+8k+4-4k-4\\&=4k^2-4k+8k\\&=8q+8k &&\text{Por hipótesis de inducción}\\&=8(q+k)\end{aligned}$$

Finalmente, $8|8(q+k)$ se verifica ya que $q+k\in\mathbb{Z}$. Por tanto, $8|(2n-1)^2-1$, para cada $n\in\mathbb{N}$.

4.2 Procederemos por inducción en n.

i) Verificamos que se cumple para $n=1$.
En efecto, $6|(1)^3-1$, es decir, $6|0$, lo cual se verifica por **(P2)**.

ii) Supongamos que se cumple para $n=k$, es decir, supongamos que $6|k^3-k$.

iii) Luego, si $n=k+1$, tenemos que

$$\begin{aligned}(k+1)^3-(k+1)&=k^3+3k^2+3k+1-k-1\\&=k^3-k+3k^2+3k\end{aligned}$$

Notemos que por hipótesis de inducción $6|k^3-k$, y si logramos demostrar que $6|3k^2+3k$, por **(P8)** garantizaríamos que $6|k^3-k+3k^2+3k$. Así, demostraremos que $6|3k^2+3k$ $\forall n\in\mathbb{N}$ por inducción en n.

i) Verificamos que se cumple para $n=1$.
Si $n=1$, tenemos que $6|3(1)^2+3(1)$, es decir, $6|6$, lo que se valida por **(P1)**.

ii) Supongamos que se cumple para $n=k$, es decir, supongamos que $6|3k^2+3k$. Lo que implica que $\exists q\in\mathbb{Z}$ tal que $6q=3k^2+3k$.

iii) Luego, si $n=k+1$, tenemos que

$$\begin{aligned}3(k+1)^2+3(k+1)&=3(k^2+2k+3)+3k+3\\&=3k^2+6k+9+3k+3\\&=6q+6k+12\\&=6(q+k+2)\end{aligned}$$

Es decir $6|6(q+k+2)$ lo cual es verdadero ya que $q+k+2\in\mathbb{Z}$. Por tanto, $6|3k^2+3k$, lo que a su vez por **(P8)**, implica que $6|n^3-n$, para cada $n\in\mathbb{N}$.

4.3 Procederemos por inducción en n.

i) Verificamos que se cumple para $n=1$.
Es claro que $9|(1)^3+(1+1)^3+(1+2)^3$, es decir, $9|1+8+27$, osea $9|36$, lo cual es verdadero.

ii) Supongamos que se cumple para $n=k$, es decir, supongamos que

$$9|k^3+(k+1)^3+(k+2)^3$$

Lo que implica que $\exists q\in\mathbb{Z}$ tal que $9q=k^3+(k+1)^3+(k+2)^3$.

iii) Luego, si $n=k+1$, tenemos que

$$\begin{aligned}(k+1)^3+\big((k+1)+1\big)^3+\big((k+1)+2\big)^3 &= (k+1)^3+(k+2)^3+(k+3)^3\\ &= (k+1)^3+(k+2)^3+k^3+9k^2+27k+27\\ &= 9q+9k^2+27k+27 && \text{Por (ii)}\\ &= 9(q+k^2+3k+3)\end{aligned}$$

Finalmente, $9|9(q+k^2+3k+3)$ se verifica ya que $(q+k^2+3k+3)\in\mathbb{Z}$. Por tanto, $9|n^3+(n+1)^3+(n+2)^3$, para cada $n\in\mathbb{N}$.

4.4 Procederemos por inducción en n.

i) Verificamos que se cumple para $n=1$.
Es claro que

$$\begin{aligned}&133|11^{1+2}+12^{2(1)+1}\\ &133|11^3+12^3\\ &133|3059\\ &133|133(23)\end{aligned}$$

ii) Supongamos que se cumple para $n=k$, es decir, supongamos que $133|11^{k+2}+12^{2k+1}$.
Lo que implica que $\exists q\in\mathbb{Z}$ tal que $133q=11^{k+2}+12^{2k+1}$.

iii) Luego, si $n=k+1$, tenemos que

$$\begin{aligned}11^{(k+1)+2}+12^{2(k+1)+1} &= 11^{k+3}+12^{2k+3}\\ &= 11^{k+2}\cdot 11+12^{2k+1}\cdot 12^2\\ &= 11^{k+2}(144-133)+12^{2k+1}\cdot 144\\ &= 144\cdot 11^{k+2}-133\cdot 11^{k+2}+144\cdot 12^{2k+1}\\ &= 144\big(11^{k+2}+12^{2k+1}\big)-133\cdot 11^{k+2}\\ &= 144(133q)-133\cdot 11^{k+2} && \text{Por hipótesis de inducción}\\ &= 133(144q-11^{k+2}).\end{aligned}$$

Finalmente, $133|133(144q-11^{k+2})$ se verifica ya que $(144q-11^{k+2})\in\mathbb{Z}$. Por tanto, $133|11^{n+2}+12^{2n+1}$, para cada $n\in\mathbb{N}$.

4.5 Notemos que

$$\begin{aligned}abcabc &= 100000a+10000b+1000c+100a+10b+c\\ &= 100100a+10010b+1001c\\ &= (1001\cdot 100)a+(1001\cdot 10)b+1001c\\ &= 1001(100a+10b+c)\\ &= 143(7)(100a+10b+c)\\ &= 143(700a+70b+7c)\end{aligned}$$

Luego, tenemos que $143|143(700a+70b+7c)$, lo cual es verdadero. Por tanto, $143|abcabc$.

5. Notemos que

$$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+...+ab^{n-2}+b^{n-1})$$

Lo cual implica que $a-b|a^n-b^n$.

6. Por el **Teorema 0.2.1** sabemos que existen $q,r\in\mathbb{Z}$ únicos tales que $a=bq+r$ con $0\leq r<|b|$. Luego,

i) Si $b|a$, entonces $\exists k \in \mathbb{Z}$ tal que $a=bk$. Notemos que $a=bk+0$. Como $a=bq+r$ y q y r son únicos, sigue que $r=0$.

ii) Si $a=bq+r$ y $r=0$, entonces $a=bq$, lo cual implica que $b|a$.

7.10 $q=m^2+2m+1$ y $r=1$.

8. **i)** Si $a \geq 0$ y $b \geq 0$, entonces $|a|=a$ y $|b|=b$. Por lo que $(a,b)=(|a|,|b|)$.

ii) Si $a \geq 0$ y $b<0$, entonces $|a|=a$ y $|b|=-b$. Sea $d=(a,b)$, entonces $d|a$ y $d|b$ por lo que $\exists q_1,q_2 \in \mathbb{Z}$ tales que $a=dq_1$ y $b=dq_2$, es decir $|a|=dq_1$ y $-b=-dq_2$, osea $|b|=d(-q_2)$, lo que implica que $d\,\Big|\,|a|$ y $d\,\Big|\,|b|$. Sigue que $(a,b)=(|a|,|b|)$.

iii) Si $a<0$ y $b<0$, entonces $|a|=-a$ y $|b|=-b$. Sea $d=(a,b)$, entonces $d|a$ y $d|b$ por lo que $\exists q_1,q_2 \in \mathbb{Z}$ tales que $a=dq_1$ y $b=dq_2$. Luego, $-a=-dq_1$ y $-b=-dq_2$, es decir, $|a|=d(-q_1)$ y $|b|=d(-q_2)$, lo que implica que $d\,\Big|\,|a|$ y $d\,\Big|\,|b|$. Por tanto, $(a,b)=(|a|,|b|)$.

9.5 Por el ejercicio 8, $(764,-866)=(764,866)$. Aplicando el algoritmo de Euclides, tenemos:

$$\begin{array}{r} 1 \\ 764\,\overline{)866} \\ \underline{764} \\ 102 \end{array} \qquad \begin{array}{r} 7 \\ 102\,\overline{)764} \\ \underline{714} \\ 50 \end{array} \qquad \begin{array}{r} 2 \\ 50\,\overline{)102} \\ \underline{100} \\ 2 \end{array} \qquad \begin{array}{r} 25 \\ 2\,\overline{)50} \\ \underline{4} \\ 10 \\ \underline{10} \\ 0 \end{array}$$

Por tanto, $2=(764,-866)$.

10. Si $(a,b)=1$, entonces $\exists s,t \in \mathbb{Z}$ tales que $1=as+bt$. Sea $c \in \mathbb{Z}$ arbitrario pero fijo, entonces $c=asc+btc$, por lo que la ecuación $c=ax+by$ tiene soluciones enteras $x=sc$ y tc.

11. **i)** Si $d=(a,b)$, entonces $d|a$ y $d|b$. Supongamos que $d\nmid c$, por el ejercicio 1.3, sigue que $\nexists x,y \in \mathbb{Z}$ tales que $c=ax+by$, entonces, por contraposición, $d|c$.

ii) Si $d=(a,b)$, entonces $\exists s,t \in \mathbb{Z}$ tales que $d=as+bt$. Si $d|c$, entonces $\exists q \in \mathbb{Z}$ tal que $c=dq$. Luego, $c=(as+bt)q$, osea $c=asq+btq$, por lo que la ecuación $c=ax+by$ tiene soluciones enteras $x=sq$ y $y=tq$.

12. Tenemos que $d|a$ y $d|b$ con $d>0$. Sea $c \in \mathbb{Z}$ tal que $c|a$ y $c|b$. Por **(P9)**, $c|as$ y $c|bt$, y por **(P8)**, $c|as+bt$. Por hipótesis $d=as+bt$, entonces $c|d$. Por tanto, $d=(a,b)$.

13. Si $d=(a,b)$ y $d=as+bt$, entonces $d|a$ y $d|b$, es decir $\exists q_1,q_2 \in \mathbb{Z}$ tales que $a=dq_1$ y $b=dq_2$. Sigue que $d=(dq_1)s+(dq_2)t$, osea $d=d(sq_1+tq_2)$. Como $d>0$, tenemos que $1=sq_1+tq_2$. Es claro que 1 es combinación lineal de s y t, además es el mínimo entero positivo que satisface esta combinación lineal, entonces $(s,t)=1$. Finalmente, la solución de **Ej. 1.2** es un contraejemplo de que s y t no son únicos.

14. Si $d=(a,b)$, entonces $\exists s,t \in \mathbb{Z}$ tales que $d=as+bt$. Además, por hipótesis, $a=dq_1$ y $b=dq_2$, lo que implica que $d=(dq_1)s+(dq_2)t$, osea $d=d(q_1s+q_2t)$. Como $d>0$, sigue que $1=q_1s+q_2t$. Es claro que 1 es combinación lineal de q_1 y q_2, y es el mínimo entero positivo que satisface esta propiedad, entonces, $(q_1,q_2)=1$.

15. Si $c|a$, entonces $\exists q \in \mathbb{Z}$ tal que $a=cq$. Además, por hipótesis $(a,b)=1$, lo que implica que $1=as+bt$. Notemos que $1=(cq)s+bt$, osea $1=c(qs)+bt$. Es claro que 1 es combinación lineal de c y b, además es el mínimo entero positivo que satisface esta combinación lineal, entonces, por el Algoritmo de Euiclides, $(b,c)=1$.

16. Si $a|c$ y $b|c$, entonces $\exists q_1,q_2 \in \mathbb{Z}$ tales que $c=aq_1$ y $c=bq_2$. Además, por hipótesis $d=(a,b)$, entonces $\exists s,t \in \mathbb{Z}$ tales que $d=as+bt$. Luego $cd=c(as+bt)$, osea $cd=asc+btc$. Notemos que $cd=as(bq_2)+bt(aq_1)$, por lo que $cd=ab(sq_2)+ab(tq_1)$. Finalmente, $cd=ab(sq_2+tq_1)$, lo cual implica que $ab|cd$.

17. Si $(a,b)=1$ entonces $1|a$ y $1|b$. Luego, por **(P9)**, $1|bc$. Además, si $\exists d \in \mathbb{Z}$ tal que $d|a$ y $d|b$, entonces tendríamos que $d|1$, y por **(P5)**, $d=\pm 1$. De este modo, $1=(a,bc)$, es decir, $(a,b)=(a,bc)$.

18. Tenemos que $\exists d=(a,b)$ y d es el mínimo entero positivo para el cual $\exists s,t \in \mathbb{Z}$ tales que $d=as+bt$. Notemos que $kd=k(as+bt)$, osea $kd=(ak)s+(bk)t$. Como $k>0$, se verifica que kd es el mínimo entero postivo que satisface una combinación lineal de ak y bk, lo que implica que $(ak,bk)=kd$, osea $(ak,bk)=k(a,b)$.

19. Tenemos que $\exists d=(a,b)$ y d es el mínimo entero positivo para el cual $\exists s,t \in \mathbb{Z}$ tales que $d=as+bt$. Por definición, $|k|\geq 0$, pero $k\neq 0$, así, se sigue que $|k|>0$. Notemos que $|k|d=|k|(as+bt)$, osea $|k|d=a|k|s+b|k|t$. Observamos que:

i) Si $k<0$, tenemos que $|k|=-k$, por lo que $|k|d=a(-k)s+b(-k)t$, es decir, $|k|d=ak(-s)+bk(-t)$.

ii) Si $k>0$, entonces $|k|=k$, por lo que $|k|d=(ak)s+(bk)t$.

En cualquier caso, se verifica que $|k|d$ es el mínimo entero postivo que satisface una combinación lineal de ak y bk, lo que implica que $(ak,\, bk)=|k|d$, osea $(ak,bk)=|k|(a,b)$.

20. Sea $k=(a+b,a-b)$, entonces $k|a+b$ y $k|a-b$, por lo que $\exists q_1,q_2 \in \mathbb{Z}$ tales que $(a+b)=kq_1$ y $(a-b)=kq_2$. Notemos que

$$\begin{aligned}(a+b)+(a-b)&=kq_1+kq_2\\ 2a&=k(q_1+q_2)\end{aligned}$$

Similarmente,

$$\begin{aligned}(a+b)-(a-b)&=kq_1-kq_2\\ 2b&=k(q_1-q_2)\end{aligned}$$

De este modo, $k|2a$ y $k|2b$, y por **(P9)** se verifica que $k|2as$ y $k|2bt$. Además, por **(P8)** se cumple que $k|2as+2bt$. Luego, por hipótesis, $1=(a,b)$, lo que implica que $\exists s,t \in \mathbb{Z}$ tales que $1=as+bt$, así $2=2as+2bt$. Finalmente, $k|2$, osea $(a+b,a-b)=1$ o 2.

21. Tenemos que $(a,b)=1$, entonces, por la proposición 0.42, $(a,b^n)=1\ \forall n \in \mathbb{N}$. Luego, $(a,b^n)=(b^n,a)$, osea $(b^n,a)=1$. De este modo, por la proposición 0.42, $(b^n,a^m)=1\ \forall m \in \mathbb{N}$. Finalmente, $(b^n,a^m)=(a^m,b^n)$, es decir, $(a^m,b^n)=1\ \forall m,n \in \mathbb{N}$.

22. Tenemos que $(a,b)=k$, entonces $k|a$ y $k|b$, por esto $\exists q_1,q_2 \in \mathbb{Z}$ tales que $a=kq_1$ y $b=kq_2$. Luego, por **Ej. 14** se verifica que $(q_1,q_2)=1$. Notemos que $a^n=(kq_1)^n$ y $b^n=(kq_2)^n$, osea $a^n=k^nq_1^n$ y $b^n=k^nq_2^n$. De este modo $(a^n,b^n)=(k^nq_1^n,\, kq_2^n)$. Luego, por **Ej. 18**, se verifica que $(k^nq_1^n,kq_2^n)=k^n(q_1^n,q_2^n)$, es decir $(a^n,b^n)=k^n(q_1^n,q_2^n)$. Como $(q_1,q_2)=1$, por **Ej. 21** tenemos que $(q_1^n,q_2^n)=1$. Finalmente, observamos que $(a^n,b^n)=k^n$.

23. Como m y n son primos relativos, entonces k^2 no es primo, lo cual implica que $\exists p_1,p_2,...,p_n$ números primos tales que $k^2=p_1^2\cdot p_2^2\cdots p_n^2$. Además $k^2=mn$, entonces $m=p_1^2\cdot p_2^2\cdots p_m^2$ y $n=p_1^2\cdot p_2^2\cdots p_l^2$. Por tanto, $m=a^2$ y $n=b^2$, para $a=p_1\cdot p_2\cdots p_m$ y $b=p_1\cdot p_2\cdots p_l$.

24. Tenemos que $(a,c)=1$ y $(b,c)=1$, entonces $\exists s,t,x,y \in \mathbb{Z}$ tales que $1=as+ct$ y $1=bx+cy$. Luego,

$as=1-ct$ y $bx=1-cy$. Notemos que

$$\begin{aligned}(as)(bx)&=(1-ct)(1-cy)\\ ab(sx)&=1-cy-ct+ctcy\\ ab(sx)&=1-c(y+t-tcy)\\ ab(sx)+c(y+t-tcy)&=1\end{aligned}$$

Es claro que 1 es combinación lineal de ab y c, y es el mínimo entero positivo que satisface esta propiedad. Por tanto, $(ab,c)=1$.

25. Si $b^2|a^2$, entonces $\exists k\in\mathbb{Z}$ tal que $a^2=b^2k$. Luego, por el teorema fundamental de la aritmética, $\exists p_1,p_2,...,p_i,q_1,q_2,...,q_j$ primos tales que $a=p_1p_2\cdots p_i$ y $b=q_1q_2\cdots q_j$. Entonces, $a^2=(p_1p_2\cdots p_i)^2$ y $b^2=(q_1q_2\cdots q_j)^2$, osea $a^2=p_1^2p_2^2\cdots p_i^2$ y $b^2=q_1^2q_2^2\cdots q_j^2$. Sigue que $p_1^2p_2^2\cdots p_i^2=kq_1^2q_2^2\cdots q_j^2$, lo que implica que k debe tener una factorización prima con potencias pares, en otras palabras, es un cuadrado perfecto. De este modo, $\sqrt{k}\in\mathbb{Z}$. Finalmente, de $a^2=b^2k$ obtenemos $a=b\sqrt{k}$, es decir, $b|a$.

26. Si $b^n|a^n$, entonces $\exists k\in\mathbb{Z}$ tal que $a^n=b^nk$. Luego, por el teorema fundamental de la aritmética podemos escribir a a y b como el producto de números primos, es decir, $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ y $b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r}$, donde $\alpha_i,\beta_i\geq 0$. Notemos que los exponentes pueden ser 0 si algún primo ocurre en la factorización de uno de los enteros a y b pero no en el otro. De este modo, $a^n=p_1^{n\alpha_1}p_2^{n\alpha_2}\cdots p_r^{n\alpha_r}$ y $b^n=p_1^{n\beta_1}p_2^{n\beta_2}\cdots p_r^{n\beta_r}$. De $a^n=b^nk$ sigue que $p_1^{n\alpha_1}p_2^{n\alpha_2}\cdots p_r^{n\alpha_r}=p_1^{n\beta_1}p_2^{n\beta_2}\cdots p_r^{n\beta_r}k$, como la factorización es única, tenemos que $n\beta_i\leq n\alpha_i$ para cada i, lo que implica que $\beta_i\leq\alpha_i$ para cada i. Por tanto, $b|a$.

27. Supongamos que $\sqrt{a}\in\mathbb{Q}$, entonces $\sqrt{a}=\frac{p}{q}$, con $p,q\in\mathbb{Z}$ y $q\neq 0$. Luego, $a=(\frac{p}{b})^2$, pero esto contradice nuestra hipótesis. Por tanto, $\sqrt{a}\notin\mathbb{Q}$.

28. Supongamos que $\sqrt[n]{a}\in\mathbb{Q}$, entonces $\sqrt[n]{a}=\frac{p}{q}$, con $p,q\in\mathbb{Z}$ y $q\neq 0$. Luego, $a=(\frac{p}{q})^n$, pero esto contradice nuestra hipótesis. Por tanto, $\sqrt[n]{a}\notin\mathbb{Q}$.

29. Primero demostraremos que $9|10^n-1\ \forall n\in\mathbb{N}$. Procederemos por inducción sobre n.

i) Verificamos que se cumple para $n=1$.
Es claro que $9|10^1-1$, osea $9|9$.

ii) Supongamos que se cumple para $n=k$, es decir, supongamos que $9|10^k-1$. Esto implica que $\exists q\in\mathbb{Z}$ tal que $10^k-1=9q$.

iii) Luego, si $n=k+1$ tenemos que

$$\begin{aligned}10^{k+1}-1&=(10)10^k-1\\ &=(9+1)10^k-1\\ &=(9)10^k+10^k-1\\ &=(9)10^k+9q && \text{Por hipótesis de inducción}\\ &=9(10^k+q)\end{aligned}$$

Sigue que $9|9(10^k+q)$, lo cual es verdadero. Por tanto, $9|10^n-1\ \forall n\in\mathbb{N}$.
Retomando que si $a_1,a_2,...,a_n$ son dígitos, el número cifrado $a_1a_2\cdots a_n$ tiene la forma

$$\begin{aligned}&10^{n-1}a_1+10^{n-2}a_2+\cdots+10^0a_n\\ &=10^{n-1}a_1+10^{n-2}a_2+\cdots+10^0a_n\\ &=\left(10^{n-1}-1\right)a_1+a_1+\left(10^{n-2}-1\right)a_2+a_2+\cdots+\left(10^0-1\right)a_n+a_n\\ &=\left(10^{n-1}-1\right)a_1+\left(10^{n-2}-1\right)a_2+\cdots+\left(10^0-1\right)a_n+a_1+a_2+\cdots+a_n\end{aligned}$$

Sea $A=\left(10^{n-1}-1\right)a_1+\left(10^{n-2}-1\right)a_2+\cdots+\left(10^0-1\right)a_n$ y $B=a_1+a_2+\cdots+a_n$.

i) Si $9|a_1a_2...a_n$. Notemos que $9|10^n-1$ $\forall n\in\mathbb{N}$, y por **(P9)** $9|(10^n-1)c$ $\forall c\in\mathbb{Z}$ y por **(P8)** $9|A$. Finalmente, por **(P13)** $9|B$, es decir, $9|a_1+a_2+\cdots+a_n$.

ii) Si $9|a_1+a_2+...a_n$. Notemos que $9|10^n-1$ $\forall n\in\mathbb{N}$, y por **(P9)** $9|(10^n-1)c$ $\forall c\in\mathbb{Z}$. Por **(P8)** $9|A$ y por hipótesis, $9|B$. Finalmente, por **(P8)** $9|A+B$, es decir, $9|a_1a_2\cdots a_n$.

30.1 Sea $d=(a_0,a_1,...,a_n)$. Si $d'=(a_0,a_1,...,a_n)$, por definición $d'|d$ y $d|d'$. Luego, por **(P6)** $d=d'$.

31. Sea $d=\big((a,b),c\big)$. Por definición, $d|(a,b)$ y $d|c$. También, $(a,b)|a$ y $(a,b)|b$. Luego, por **(P8)** $d|a$ y $d|b$. Luego, sea $d'\in\mathbb{Z}$ tal que $d'|a,b,c$, entonces $d'|(a,b)$. De este modo, $d'|d$. Por tanto, $((a,b),c)=(a,b,c)$.

32. Sea $d=(a_1,a_2,...,a_n)$ y $d'=\big(|a_1|,|a_2|,...,|a_n|\big)$, entonces $d\Big|a_1,a_2,...,a_n$ y $d'\Big||a_1|,|a_2|,...,|a_n|$. Por **(P12)** se verifica que $d\Big||a_1|,|a_2|,...,|a_n|$ y $d'\Big|a_1,a_2,...,a_n$, lo que implica que $d|d'$ y $d'|d$. Finalmente, por **(P6)** $d=d'$, es decir, $(a_1,a_2,...,a_n)=\big(|a_1|,|a_2|,...,|a_n|\big)$.

33.1 Sea $m=[a,b]$ y $m'=[a,b]$, entonces $a|m$ y $b|m$. También, $a|m'$ y $b|m'$. Por definición, $m|m'$ y $m'|m$. Finalmente, por **(P6)** $m=m'$.

33.2 Sea $A=\{x\in\mathbb{N}:\ a|x \text{ y } b|x\}$. Claramente, $a|ab$ y $b|ab$, entonces $\exists q_1,q_2\in\mathbb{Z}$ tales que $ab=aq_1$ y $ab=aq_2$. Luego,

i) Si $ab\geq 0$, entonces $|ab|=ab$, por lo que $a\big||ab|$ y $b\big||ab|$.

ii) Si $ab<0$, entonces $|ab|=-ab$. Notemos que $-ab=-aq_1$ y $-ab=-bq_2$. Entonces, $|ab|=a(-q_1)$ y $|ab|=b(-q_2)$, lo que implica que $a\big|ab|$ y $a\big||ab|$.

De este modo, $|ab|\in A$. Así $A\neq\emptyset$ y por el principio del buen orden, A contiene un elemento mínimo m. Supongamos que $\exists s$ tal que $a|s$ y $b|s$. Por el algoritmo de la división, $\exists q,r\in\mathbb{Z}$, únicos tales que

$$s=mq+r \text{ con } 0\leq r<|m|$$

Sigue que, $r=s-mq$. Observemos que

i) Como $a|m$ y $a|s$, $\exists k_1,k_2\in\mathbb{Z}$ tales que $m=ak_1$ y $s=ak_2$, luego $mq=ak_1q$. Notemos que $s-mq=ak_2-ak_1q$, es decir, $r=a(k_2-k_1q)$, lo cual implica que $a|r$.

ii) Como $b|m$ y $b|s$, $\exists k_3,k_4\in\mathbb{Z}$ tales que $m=bk_3$ y $s=bk_4$, luego $mq=bk_4q$. Notemos que $s-m=bk_3-bk_4q$, es decir, $r=b(k_3-k_4q)$, lo cual implica que $b|r$.

Tenemos que $m\in\mathbb{N}$, entonces $|m|=m$. Así $0\leq r<m$. Observemos que si $0<r<m$, entonces $r\in A$ y se contradice que m es elemento mínimo de A, por lo que $r=0$. Finalmente, $s=mq$. Por tanto $m|s$.

33.3 Sea $m=[a,b]$ y $m'=\big[|a|,|b|\big]$, entonces $a|m$ y $b|m$. También $|a|\big|m'$ y $|b|\big|m'$. Por **(P12)** se verifica que $|a|\big|m$ y $|b|\big|m$. Por definición, $m|m'$ y $m'|m$. Finalmente, por **(P6)**, $m=m'$, es decir, $[a,b]=\big[|a|,|b|\big]$.

33.4 Sea $m=[a,b]$ y d tal que $md=ab$. Tenemos que $a|m$, entonces $\exists s,t\in\mathbb{Z}$ tales que $m=as$ y $m=bt$. Luego, $md=asd$ y $md=btd$, entonces $ab=asd$ y $ab=btd$. Sigue que $a=td$ y $b=sd$, lo que implica que $d|a$ y $d|b$. Sea $d'\in\mathbb{Z}$ tal que $d'|a$ y $d'|b$, entonces $\exists a',b'\in\mathbb{Z}$ tales que $a=d'a'$ y $b=d'b'$. Definamos $m'=a'b'd'$, así tenemos $m'=ab'$ y $m'=a'b$, lo que implica que $a|m'$ y $b|m'$. Por definición, $m|m'$, entonces $\exists q\in\mathbb{Z}$ tal que $m'=mq$. Luego, $m'd'=mqd'$, es decir, $m'd'=a'b'd'd'$, osea $m'd'=ab$ y $m'd'=md$. De este moodo, $mqd'=md$, de donde se sigue que $qd'=d$, lo que implica que $d'|d$. Entonces, $d=(a,b)$. Finalmente, como $md=ab$, $[a,b](a,b)=ab$. Por tanto, $[a,b]=\frac{a\cdot b}{(a,b)}$.

33.5 Notemos que

$$
\begin{aligned}
[ak,bk] &= \frac{ak\cdot bk}{(ak,bk)} && \text{Por el ejercicio 33.4}\\
&= \frac{ak\cdot bk}{k(a,b)} && \text{Por el ejercicio 18}\\
&= \frac{k^2\cdot ab}{k(a,b)}\\
&= k\frac{ab}{(a,b)}
\end{aligned}
$$

Luego,

$$
\begin{aligned}
[a,b] &= \frac{a\cdot b}{(a,b)} && \text{Por el ejercicio 33.4}\\
k[a,b] &= k\frac{a\cdot b}{(a,b)}
\end{aligned}
$$

Por tanto, $[ak,bk]=k[a,b]$.

37. Notemos que $p|a_1(a_2\cdot\ldots\cdot a_n)$.

$$
\begin{gathered}
\text{Si } p|a_1 \text{ se cumple nuestra tesis. Si } p\nmid a_1\text{, entonces } p|a_2\cdot\ldots\cdot a_n\\
\text{Si } p|a_2 \text{ se cumple nuestra tesis. Si } p\nmid a_2\text{, entonces } p|a_3\cdot\ldots\cdot a_n\\
\vdots\\
\text{Si } p|a_{n-1} \text{ se cumple nuestra tesis. Si } p\nmid a_{n-1}\text{, entonces } p|a_n
\end{gathered}
$$

Por tanto, $p|a_i$ para algún $i=1,2,\ldots,n$.

38. Si $a<-1$, entonces $-a>1$. Por el teorema fundamental de la aritmética, $-a=p_1\cdot p_2\cdot\ldots\cdot p_n$. Por tanto, $a=-p_1\cdot p_2\cdots p_n$.

40 Supongamos que n no es primo, entonces $\exists m,k\in\mathbb{Z}^+-\{0\}$ con $m,k>1$ tales que $n=mk$. De este modo

$$
\begin{aligned}
2^n-1 &= 2^{mk}-1\\
&= (2^k)^m-1^m\\
&= (2^k-1)\left(\left(2^k\right)^{m-1}+\left(2^k\right)^{m-2}+\cdots+\left(2^k\right)^0\right)
\end{aligned}
$$

Notemos que $m,k>1$, entonces $2^k-1>1$ y $\left(\left(2^k\right)^{m-1}+\left(2^k\right)^{m-2}+\cdots+\left(2^k\right)^0\right)>1$.
Sea $q_1=2^k-1$ y $q_2=\left(\left(2^k\right)^{m-1}+\left(2^k\right)^{m-2}+\cdots+\left(2^k\right)^0\right)$. Entonces $2^n-1=q_1q_2$ con $q_1,q_2\in\mathbb{Z}^+-\{0\}$.
Por tanto, 2^n-1 no es primo.

43. Tenemos que p es primo, entonces los únicos divisores de p^{n-1} son $p^{n-1},p^{n-2},\ldots,1$. Luego, $p^{n-1}=(p-1)\left(p^{n-1}+p^{n-2}+\cdots+1\right)$. De este modo, $\frac{p^{n-1}}{p-1}=\left(p^{n-1}+p^{n-2}+\cdots+1\right)$. Por tanto, la suma de divisores positivos de p^{n-1} es igual a $\frac{p^{n-1}}{p-1}$.

44. Supongamos que el conjunto de los números primos es finito. Definamos a P como el conjunto de los números primos. Tenemos que $P=\{2,3,\ldots,p_n\}$ para algún $n\in\mathbb{N}$. Luego, sea $a=2\cdot3\cdot\ldots\cdot p_n$, vemos que $2|a,3|a,\ldots,p_n|a$. Tomemos $a+1$, para el cual tenemos que $2\nmid a,3\nmid a,\ldots,p_n\nmid a$. Entonces, $a+1\in P$, lo cual es una contradicción. Por tanto, el conjunto de los números primos no es finito.

Proposición 1.4.2

Si z_1 y z_2 son complejos, entonces:

i) $\overline{(\overline{z_1})}=z_1$.

ii) $\overline{z_1+z_2}=\overline{z_1}+\overline{z_2}$.

iii) $\overline{z_1\cdot z_2}=\overline{z_1}\cdot\overline{z_2}$.

iv) $\overline{z_1-z_2}=\overline{z_1}-\overline{z_2}$.

Demostración

Sea $z_1=a+bi$ t $z_2=c+di$.

i)

$$\begin{aligned}\overline{(\overline{z_1})}&=\overline{(\overline{a+bi})}\\&=\overline{(a-bi)}\\&=a-(-bi)\\&=a+bi\\&=z_1\end{aligned}$$

ii)

$$\begin{aligned}\overline{z_1+z_2}&=\overline{(a+bi)+(c+di)}\\&=\overline{(a+c)+(b+d)i}\\&=(a+c)-(b+d)i\\&=a-bi+c-di\\&=\overline{z_1}+\overline{z_2}\end{aligned}$$

iii)

$$\begin{aligned}\overline{z_1\cdot z_2}&=\overline{(a+bi)\cdot(c+di)}\\&=\overline{(ac-bd)+(ad+bc)i}\\&=(ac-bd)-(ad+bc)i\\&=(ac-bd)+(-ad-bc)i\\&=(a-bi)\cdot(c-di)\\&=\overline{z_1}\cdot\overline{z_2}\end{aligned}$$

iv)

$$\begin{aligned}\overline{z_1 - z_2} &= \overline{(a+bi)-(c+di)}\\ &= \overline{a+bi-c-di}\\ &= \overline{(a-c)+bi-di}\\ &= \overline{(a-c)+(b-d)i}\\ &= (a-c)-(b-d)i\\ &= a-c-bi+di\\ &= (a-bi)-(c-di)\\ &= \overline{z_1}-\overline{z_2}\end{aligned}$$

Observación.

i) $z \cdot \overline{z} = a^2 + b^2$.

ii) $|z| = \sqrt{z \cdot \overline{z}}$.

iii) $|z|^2 = z \cdot \overline{z}$.

iv) $z + \overline{z} = 2Re(z)$.

v) $Re(z) \leq |z|$

vi) $\overline{z_1 \cdot \overline{z_2}} = \overline{z_1} \cdot z_2$.

Demostración.

i)

$$\begin{aligned}z \cdot \overline{z} &= (a+bi)(a-bi)\\ &= a^2+b^2-abi+abi\\ &= a^2+b^2\end{aligned}$$

ii)

$$\begin{aligned}|z| &= \sqrt{a^2+b^2}\\ &= \sqrt{z \cdot \overline{z}}\end{aligned}$$

iii)

$$\begin{aligned}|z|^2 &= \left(\sqrt{z \cdot \overline{z}}\right)^2\\ &= z \cdot \overline{z}\end{aligned}$$

iv)

$$\begin{aligned}z + \overline{z} &= (a+bi)+(a-bi)\\ &= 2a\end{aligned}$$

v) $\forall a \in \mathbb{R}, a \leq |a| = \sqrt{a^2} \leq \sqrt{a^2+b^2}$, entonces

vi)

$$\begin{aligned}\overline{z_1}\cdot\overline{z_2}&=\overline{z_1}\cdot\overline{\overline{z_2}}\\&=\overline{z_1}\cdot z_2\end{aligned}$$

Proposición 1.4.3

Si z_1 y z_2 son complejos, entonces:

i) $|z_1|=0$, si y solo si, $z_1=0$.

ii) $|\overline{z_1}|=|z_1|$.

iii) $|z_1\cdot z_2|=|z_1|\cdot|z_2|$.

iv) $|z_1+z_2|\leq|z_1|+|z_2|$

v) Si $z_2\neq 0$, $|\frac{z_1}{z_2}|=\frac{|z_1|}{|z_2|}$.

vi) $|z_1|-|z_2|\leq|z_1-z_2|$.

demostración

i) **a)**

$$\begin{aligned}|z_1|&=0\\|a+bi|&=0\\\sqrt{a^2+b^2}&=0\\a^2+b^2&=0\\a^2&=-b^2\end{aligned}$$

Como $a,b\in\mathbb{R}$ y $x^2\geq 0$ $\forall x\in\mathbb{R}$, sigue que $a=0$ y $b=0$, por tanto $z_1=0$.

b) Si $z_1=0$, es inmediato que $|z_1|=0$.

ii)

$$\begin{aligned}|\overline{z_1}|&=|a-bi|\\&=|a+(-b)i|\\&=\sqrt{a^2+(-b)^2}\\&=\sqrt{a^2+b^2}\\&=|z_1|\end{aligned}$$

iii)

$$\begin{aligned}|z_1\cdot z_2|^2&=(z_1\cdot z_2)(\overline{z_1\cdot z_2})\\&=(z_1\cdot z_2)(\overline{z_1}\cdot\overline{z_2})\\&=(z_1\overline{z_1})\cdot(z_2\overline{z_2})\\&=|z_1|^2\cdot|z_2|^2\end{aligned}$$

Notemos que $|z|\geq 0$ $\forall z\in\mathbb{C}$. Por tanto, $|z_1\cdot z_2|=|z_1|\cdot|z_2|$.

iv)

$$
\begin{aligned}
|z_1+z_2|^2 &= (z_1+z_2)(\overline{z_1+z_2}) \\
&= (z_1+z_2)(\overline{z_1}+\overline{z_2}) \\
&= z_1\cdot\overline{z_1}+z_1\cdot\overline{z_2}+z_2\overline{z_1}+z_2\cdot\overline{z_2} \\
&= |z_1|^2+z_1\cdot\overline{z_2}+z_2\cdot\overline{z_1}+|z_2|^2 \\
&= |z_1|^2+z_1\cdot\overline{z_2}+\overline{\overline{z_2}}\cdot\overline{z_1}+|z_2|^2 \\
&= |z_1|^2+z_1\cdot\overline{z_2}+\overline{\overline{z_2}\cdot z_1}+|z_2|^2 \\
&= |z_1|^2+2Re(z_1\cdot\overline{z_2})+|z_2|^2
\end{aligned}
$$

Notemos que

v)