DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Práctica 4

2do cuatrimestre 2021 Álgebra I

Integrante	LU	Correo electrónico
Yago Pajariño	546/21	ypajarino@dc.uba.ar

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2610 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (++54 +11) 4576-3300
http://www.exactas.uba.ar

Índice

4. Práctica 4

Resumen de propiedades de divisibilidad.

1. $\forall d \in \mathbb{Z} : d \neq 0 \implies d|0$
2. $d|a \iff \pm d| \pm a \iff |d|||a|$
3. $a \neq 0 : d|a \implies |d| \leq |a|$
4. $Inv(\mathbb{Z} = \{\pm 1\})$
5. $d|a \wedge a|d \iff |d| = |a|$
6. $a \in \mathbb{Z}; \pm 1|a \wedge \pm a|a$
7. $d|a \wedge d|b \implies d|(a+b)$
8. $d|a \implies d|c \cdot a$
9. $d|a \wedge d|b \implies d^2|ab$

4.1. Ejercicio 1

1. $ab|c \iff c = k \cdot ab \implies c = (kb) \cdot a \implies a|c$ Verdadera
2. $a^2 = 4k \implies a^2 = 2 \cdot (2k) \implies 2|a^2 \implies 2|a$ Verdadera
3. $2 \not| a \wedge 2 \not| a \implies (2n+1)(2m+1) = 2k$. Pero el termino de la izq es impart y el de la dercha par. ABS. Verdadera.
4. $9|3.3$ pero $9 \not| 3$ Falso
5. $2|3+3$ pero $2 \not| 3$ Falso
6. $4|4 \wedge 2|4$ pero $8 \not| 4$ Falso
7. $-2|4$ pero $-2 > 4$ Falso
8. Verdadera. Probado en teórica 10.
9. Verdadera. $a|a \implies a|a^2 \implies a|b + a^2 - a^2 \implies a|b$
10. Verdadera. Probado en teórica 10.

4.2. Ejercicio 2

4.2.A. Pregunta i

$$\begin{aligned} 3n-1|n+7 &\implies 3n-1|3n-1 \wedge 3n-1|n+7 \\ &\implies 3n-1|(-1)(3n-1)+3(n+7) \\ &\implies 3n-1|-3n+1+3n+21 \\ &\implies 3n-1|22 \end{aligned}$$

Luego $3n-1 \in Div_+(22) \iff 3n-1 \in \{1, 2, 11, 22\}$

(a) $3n-1 = 1 \implies n = \frac{2}{3} \notin \mathbb{N}$ NO

(b) $3n-1 = 2 \implies n = 1$ luego $2|8$ SI

(c) $3n-1 = 11 \implies n = 4$ luego $11|11$ SI

(d) $3n-1 = 22 \implies n = \frac{23}{3} \notin \mathbb{N}$ NO

Rta.: $n \in \{1, 4\}$

4.2.B. Pregunta ii

$$\begin{aligned} 3n-2|5n-8 &\implies 3n-2|5n-8 \wedge 3n-2|3n-2 \\ &\implies 3n-2|-3(5n-8)+5(3n-2) \\ &\implies 3n-2|4 \end{aligned}$$

Luego $3n-2 \in Div_+(4) \iff 3n-2 \in \{1,2,4\}$

(a) $3n-2=1 \implies n=\frac{-1}{3} \notin \mathbb{N}$

(b) $3n-2=2 \implies n=\frac{4}{3} \notin \mathbb{N}$

(c) $3n-2=4 \implies n=4$ y además $3.2-2|5.2-8 \iff 4|12$

Rta.: $n=2$

4.2.C. Pregunta iii

$$\begin{aligned} 2n+1|n^2+5 &\implies 2n+1|n^2+5 \wedge 2n+1|2n+1 \\ &\implies 2n+1|2(n^2+5)+(-n)(2n+1) \\ &\implies 2n+1|10-n \wedge 2n+1|2n+1 \\ &\implies 2n+1|2(10-n)+2n+1 \\ &\implies 2n+1|21 \end{aligned}$$

Luego $2n+1 \in Div_+(21) \iff 2n+1 \in \{1,3,7,21\}$

(a) $2n+1=1 \implies n=0 \notin \mathbb{N}$

(b) $2n+1=3 \implies n=1$ y $3|6$

(c) $2n+1=7 \implies n=3$ y $7|14$

(d) $2n+1=21 \implies n=10$ y $21|105$

Rta.: $n \in \{1,3,10\}$

4.2.D. Pregunta iv

$$\begin{aligned} n-2|n^3-8 &\implies n-2|n^3-8 \wedge n-2|n-2 \\ &\implies n-2|n^3-8+(-n^2)(n-2) \\ &\implies n-2|n^3-8-n^3+2n^2 \\ &\implies n-2|-8+2n^2 \wedge n-2|n-2 \\ &\implies n-2|2n^2-8+(-2n)(n-2) \\ &\implies n-2|2n^2-8+-2n^2+4n \\ &\implies n-2|-8+4n \wedge n-2|n-2 \\ &\implies n-2|-8+4n-4n+8 \\ &\implies n-2|0 \end{aligned}$$

Rta.: $n \in \mathbb{N}$

4.3. Ejercicio 3

4.3.A. Pregunta i

Demostración por inducción.

Defino $p(n) : a - b | a^n - b^n ; \forall n \in \mathbb{N}$

Caso base n=1

$p(1) : a - b | a - b \iff a - b = k(a - b); k \in \mathbb{Z}$

Dado que $k = 1$ lo cumple, $p(1)$ es verdadero.

Paso inductivo

Dado $k \geq 1$ quiero probar que $p(k) \implies p(k+1)$

HI: $a - b | a^k - b^k$

Qpq: $a - b | a^{k+1} - b^{k+1} \iff a - b | a^k \cdot a - b^k \cdot b$

Por ejercicio 8 de la guía 2: $a^n - b^n = (a - b) \cdot \sum_{i=1}^{n} \cdot a^{i-1} \cdot b^{n-i}$

Es decir, existe $x \in \mathbb{Z}$ tal que $a^n - b^n = (a - b) \cdot x$ como se quería probar.

Luego $p(n)$ es verdadero $\forall n \in \mathbb{N}$

4.3.B. Pregunta ii

$a + b = a - (-b) \implies a - (-b) | a^n - (-b)^n \implies a + b | a^n - b^n$

4.3.C. Pregunta iii

$a + b = a - (-b) \implies a - (-b) | a^n - (-b)^n \implies a + b | a^n + b^n$

4.4. Ejercicio 4

Por inducción.

Defino $p(n) : 2^{n+2} | a^{2^n} - 1 ; \forall n \in \mathbb{N}$

Caso base n=1

$p(1) : 2^{1+2} | a^{2^1} - 1 \iff 2^3 | a^2 - 1 \iff 8 | a^2 - 1$

Se que a es un entero immpar, luego $a = 2k + 1; k \in \mathbb{Z}$

Por lo tanto,

$$\begin{aligned}
8 | a^2 - 1 &\iff 8 | (2k+1)^2 - 1 \\
&\iff 8 | 4k^4 + 4k + 1 - 1 \\
&\implies 8 | 4k^2 + 4k \\
&\implies 8 | 4(k^2 + k) \\
&\iff 4(k^2 + k) = 8 \cdot m; m \in \mathbb{Z} \\
&\iff k^2 + k = 2 \cdot m \\
&\iff k(k+1) = 2 \cdot m
\end{aligned}$$

Que es verdadero pues el producto de par e impar es siempre verdadero.

Paso inductivo

Dado $k \geq 1$ quiero probar que $p(k) \implies p(k+1)$

HI: $2^{k+2} | a^{2^k} - 1$

Qpq: $2^{k+3}|a^{2^{k+1}}-1$

Pero,

$$\begin{aligned}
2^{k+2}|a^{2^k}-1 &\implies 2^{k+3}|2(a^{2^k}-1) \\
&\implies 2^{k+4}|2(a^{2^k}-1)(a^{2^k}+1) \\
&\implies 2^{k+4}|2(a^{2^{k+1}}-1) \\
&\implies 2^{k+3}|a^{2^{k+1}}-1
\end{aligned}$$

Luego $p(n)$ es verdadero, $\forall n \in \mathbb{N}$

4.5. Ejercicio 5

TODO

4.6. Ejercicio 6

4.6.A. Pregunta i

$n!|\prod_{i=n_0}^{n_0+n-1} \iff \prod_{i=n_0}^{n_0+n-1} = k \cdot n!$

Pero,

$$\begin{aligned}
\prod_{i=n_0}^{n_0+n-1} &= n_0 \cdot (n_0+1) \cdot ... \cdot (n_0+n-2) \cdot (n_0+n-1) \\
&= \frac{(n_0+n-1)!}{(n_0-1)!}
\end{aligned}$$

Recordando el número combinatorio,

$\prod_{i=n_0}^{n_0+n-1} = \binom{n_0+n-1}{n} \cdot n!$

Y dado que el combinatorio $\in \mathbb{Z}$, $n!|\prod_{i=n_0}^{n_0+n-1}$ como se quería probar.

4.6.B. Pregunta ii

$$\begin{aligned}
2|\binom{2n}{n} &\iff 2|\frac{2n!}{n! \cdot n!} \\
&\iff \frac{2n!}{n! \cdot n!} = 2k \\
&\iff \frac{2n \cdot (2n-1)!}{n! \cdot n!} = 2k \\
&\iff \frac{n \cdot (2n-1)!}{n! \cdot n!} = k
\end{aligned}$$

Luego debo probar que $k \in \mathbb{Z}$

$$\begin{aligned}
k \in \mathbb{Z} &\iff n! \cdot n!|n \cdot (2n-1)! \\
&\iff n!|\frac{(2n-1)!}{(n-1)!}
\end{aligned}$$

Por ejercicio 6.1 esto se cumple, por lo tanto $k \in \mathbb{Z}$ como se quería probar.

Y así, $\binom{2n}{n}$ es divisible por 2.

4.7. Ejercicio 7

4.7.A. Pregunta i

$$\begin{aligned} 99|10^{2n}+197 &\iff 10^{2n} \equiv -197(99) \equiv 1(99) \\ &\iff 100^n \equiv 1(99) \iff 1^n \equiv 1(99) \iff 1 \equiv 1(99) \end{aligned}$$

Que es verdadero, $\forall n \in \mathbb{N}$

4.7.B. Pregunta ii

$$\begin{aligned} 9|7 \cdot 5^{2n} + 2^{4n+1} &\iff 7 \cdot 25^n + 2 \cdot 16^n \equiv 0(9) \\ &\iff 7 \cdot 16^n + 2 \cdot 16^n \equiv 0(9) \\ &\iff 16^n \cdot 9 \equiv 0(9) \\ &\iff 16^n \cdot 0 \equiv 0(9) \\ &\iff 0 \equiv 0(9) \end{aligned}$$

Que es verdadero, $\forall n \in \mathbb{N}$

4.7.C. Pregunta iii

$$\begin{aligned} 56|13^{2n} + 28 \cdot n^2 - 84n - 1 &\iff 13^{2n} + 28n^2 + 84n \equiv 1(56) \\ &\iff 1^n + 28n^2 + 28n \equiv 1(56) \\ &\iff 28(n^2+n) \equiv 0(56) \\ &\iff 2 \cdot 28(n^2+n) \equiv 2 \cdot 0(56) \\ &\iff 56(n^2+n) \equiv 0(56) \\ &\iff 0(n^2+n) \equiv 0(56) \\ &\iff 0 \equiv 0(56) \end{aligned}$$

Que es verdadero, $\forall n \in \mathbb{N}$

4.7.D. Pregunta iv

TODO

4.8. Ejercicio 8

1. $133 = (-9) \cdot (-14) + 7$
2. $13 = 0 \cdot 111 + 13$
3. $\begin{cases} c = 4; r = (b-7) & 1 \leq b \leq 7 \\ c = 3; r = 7 & \text{otherwise} \end{cases}$
4. TODO
5. TODO
6. TODO

4.9. Ejercicio 9

Se que $a \equiv 5(18)$

1. $a^2 - 3a + 11 \equiv 5^2 - 15 + 11 \equiv 25 + 3 + 11 \equiv 3(18)$
2. $a \equiv 5(18) \implies a \equiv 5(3) \iff a \equiv 2(3)$
3. $a \equiv 5(18) \implies a \equiv 5(9)$ luego $4a + 1 \equiv 4.5 + 1 \equiv 21 \equiv 3(9)$
4. Se que $a \equiv 5(18) \implies a = 18k + 5$

$$\begin{aligned} 7a^2 + 12 &= 7(18k+5)^2 + 12 \\ &= 7 \cdot (324k^2 + 180k + 25) + 12 \\ &= 2268k^2 + 1260k + 175 + 12 \\ &= 2268k^2 + 1260k + 187 \\ &\equiv 0k^2 + 0k + 19 \equiv 19(28) \end{aligned}$$

4.10. Ejercicio 10

4.10.A. Pregunta i

$a \equiv 22 \equiv 8(14)$
$a \equiv 8(14) \implies a \equiv 8(7) \equiv 1(7)$
$a \equiv 8(14) \implies a \equiv 8(2) \equiv 0(2)$

4.10.B. Pregunta ii

$a \equiv 13 \equiv 3(5)$
$33a^3 + 3a^2 - 197a + 5 \equiv 3 \cdot 3^3 + 3 \cdot 3^2 - 197 \cdot 3 + 5 \equiv 3.2 + 3.4 - 2.3 + 2 \equiv 4(5)$

4.10.C. Pregunta iii

Pruebo con algunos casos:

1. n = 1: $S(1) = -1$
2. n = 2: $S(2) = -1 + 2 = 1$
3. n = 3: $S(3) = -1 + 2 - 6 = -5$
4. n = 4: $S(4) = -1 + 2 - 6 + 24 = 19 \equiv 7(12)$
5. n = 5: $S(5) = -1 + 2 - 6 + 24 - 120 = -101 \equiv 7(12)$

Veo que a partir de n = 4, la congruencia es igual a cero. Pues en el factorial encuentro $n.(n-1)....4.3...$
Por lo tanto $r_{12}(S(n \geq 4)) = 7$
Asi, los posibles restos son:

1. n = 1. $r_{12}(S(1)) = 11$
2. n = 2. $r_{12}(S(2)) = 1$
3. n = 3. $r_{12}(S(3)) = 7$
4. n = 4. $r_{12}(S(4)) = 7$

4.11. Ejercicio 11

Estos ejercicios se resuelven con tablas de restos de forma trivial.

4.11.A. Pregunta i

$r_5(a)$	0	1	2	3	4
$r_5(a^2)$	0	1	4	4	1

4.11.B. Pregunta ii

$r_7(a)$	0	1	2	3	4	5	6
$r_7(a^2)$	0	1	4	2	2	4	1
$r_7(a^3)$	0	1	1	6	1	6	6

No existe a tal que $r_3(a^3) = 4$

4.11.C. Pregunta iii

$r_7(a)$	0	1	2	3	4	5	6
$r_7(a^7)$	0	1	2	3	4	5	6

4.11.D. Pregunta iv

$r_7(b)$ \ $r_7(a)$	0	1	2	3	4	5	6
0	$\boxed{0}$	1	4	2	2	4	1
1	1	1	5	3	3	5	2
2	4	5	1	6	6	2	5
3	2	3	6	4	4	6	3
4	2	3	6	4	4	6	3
5	4	5	2	6	6	1	5
6	1	2	5	3	3	5	2

4.11.E. Pregunta v

TODO

4.12. Ejercicio 12

1. $2^{5k} \equiv 1(31) \implies 32^k \equiv 1^k \equiv 1(31)$
2. $2^{51833} \equiv 2^{5 \cdot 10366+3} \equiv (2^5)^{10366} \cdot 2^3 \equiv 1^{10366} \cdot 8 \equiv 8(31)$
3. $2^k \equiv 8(31) \iff 2^{5k+n} \equiv 8(31) \iff 1^k \cdot 2^n \equiv 8(31) \iff 2^n \equiv 8(31) \implies n = 3 = r_5(k)$
4. $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999} \equiv 12 \cdot 8 + 11 \cdot 25 + (-1)^{999} \equiv 3 + 27 - 1 \equiv 29(31)$

4.13. Ejercicio 13

Por inducción.

Defino $p(n) : a_n \equiv 3^n(7); \forall n \in \mathbb{N}$

Casos base n = 1; n = 2

$p(1) : a_1 \equiv 3^1(7) \equiv 3(7)$

$p(2) : a_2 \equiv 3^2(7) \equiv 2(7) \equiv -5(7)$

Luego $p(1); p(2)$ son verdaderas.

Paso inductivo Dado $k \geq 2$ quiero probar que $(p(k) \wedge p(k+1)) \implies p(k+2)$

HI: $a_k \equiv 3^k(7)$ y $a_{k+1} \equiv 3^{k+1}(7)$

Qpq: $a_{k+2} \equiv 3^{k+2}(7) \iff a_{k+2} \equiv 3^k \cdot 9 \equiv 3^k \cdot 2$

Pero,

$$\begin{aligned} a_{k+2} &= a_{k+1} - 6^{2k} \cdot a_k + 21^k \cdot k^{21} \\ &\equiv 3^{k+1} - 6^{2k} \cdot 3^k + 21^k \cdot k^{21}(7) \\ &\equiv 3^k \cdot 3 - 3^k(7) \\ &\equiv 3^k \cdot (3-1)(7) \\ &\equiv 3^k \cdot 2(7) \end{aligned}$$

Luego $(p(k) \wedge p(k+1)) \implies p(k+2)$ y por lo tanto $p(n)$ es verdadero, $\forall n \in \mathbb{N}$

4.14. Ejercicio 14

4.14.A. Pregunta i

1. $1365 = (0101010101)_2$
2. $2800 = (101011110000)_2$
3. $2 \cdot 2^{13} = (110000000000000)_2$
4. TODO

4.14.B. Pregunta ii

$$\begin{aligned} 2800 &= 175 \cdot 16 + \mathbf{0} \\ 175 &= 10 \cdot 16 + \mathbf{15} \\ 10 &= 0 \cdot 16 + \mathbf{10} \end{aligned}$$

$2800 = (AF0)_{16}$

4.15. Ejercicio 15

Multiplicar por dos a un número binario, hace que se sume uno al exponente de cada término (pensando como la sumatoria decimal de potencias de 2)

En la secuencia binaria, esto hace que se corran hacia la izq los digitos.

La división por dos hace lo mismo pero restando, generando un corrimiento hacia la derecha.

4.16. Ejercicio 16

Para demostrar los criterios de divisibilidad defino $D = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + ... + r_1 \cdot 10 + r_0$ el desarrollo decimal de un número entero positivo.

4.16.A. Divisiblidad por 8

$D \equiv r_n \cdot 2^n + r_{n-1} \cdot 2^{n-1} + ... + r_1 \cdot 2 + r_0(8)$

Se que $2^3 \equiv 0(8)$ luego todos los términos de D con $n \geq 3$ van a ser congruentes a 0 mod 8.

Luego $D \equiv r_2 \cdot 2^2 + r_1 \cdot 2 + r_0 \equiv r_2 \cdot 4 + r_1 \cdot 2 + r_0$

Por lo tanto $8|D \iff d_2 \cdot 4 + d_1 \cdot 2 + d_0 \equiv 0(8)$ con d_i es i-ésimo digito de der a izq.

4.16.B. Divisiblidad por 9

$D \equiv r_n \cdot 1^n + r_{n-1} \cdot 1^{n-1} + ... + r_1 \cdot 1 + r_0(9)$
$D \equiv r_n + r_{n-1} + ... + r_1 + r_0(9)$

Es decir que $9|D \iff \sum_{i=0}^{n} d_i \equiv 0(9)$

Coloquialmente, la suma de los dígitos de D es divisible por 9.

4.17. Ejercicio 17

4.17.A. Pregunta i

$$\begin{aligned}
k = (aaaa)_7 &\implies k = a \cdot 7^3 + a \cdot 7^2 + a \cdot 7 + a \\
&\implies k = a(7^3 + 7^2 + 7 + 1) \\
&\implies k \equiv a(7 + 1 + 7 + 1)(8) \\
&\implies k \equiv 16a \equiv 0(8)
\end{aligned}$$

4.17.B. Pregunta ii

Para $d \equiv 0(2)$ pues las potencias impares de 7 $\implies 7^{2n+1} \equiv 7(8)$ y las pares $\implies 7^{2n} \equiv 1(8)$

Así, $1 + 7 = 8 \equiv 0(8) \iff 8|k$

4.18. Ejercicio 18

1. $(2532 : 63) = 3$ y $3 = -5 \cdot 2532 + 201 \cdot 63$
2. $(131 : 23) = 1$ y $1 = -10 \cdot 131 + 57 \cdot 23$
3. TODO

4.19. Ejercicio 19

Por algoritmo de Euclides se que $(a : b) = (b : r_b(a))$

Luego $(a : b) = (b : 27) \iff (a : b) = (27 : r_{27}(b)) = (27 : 21) = 3$

4.20. Ejercicio 20

4.20.A. Pregunta i

Sea d tal que $(5a + 8 : 7a + 3) = d$

Por propiedades del MCD se que: $(d|5a + 8) \wedge (d|7a + 3) \iff d|7(5a + 8) - 5(7a + 3) \iff d|35a + 56 - 35a - 15 \iff d|41$

Luego $d \in Div_+(41) \iff d \in \{1, 41\}$ como se quería probar.

a = 1 $\implies (13 : 10) = 1$ a = 23 $\implies (123 : 164) = 41$

4.20.B. Pregunta ii

Sea d tal que $(2a^2 + 3a - 1 : 5a + 6) = d$

Por propiedades del MCD se que: $(d|2a^2 + 3a - 1) \wedge (d|5a + 6) \implies d|5(2a^2 + 3a - 1) - 2(5a + 6) \iff d|3a - 5 \implies d| - 5(3a - 5) + 3(5a + 6) \iff d| - 15a + 25 + 15a + 18 \iff d|43$

Luego $d \in Div_+(43) \iff d \in \{1, 43\}$ como se quería probar.

a = 1 $\implies (4 : 11) = 1$ a = 16 $\implies (559 : 86) = 43$

4.20.C. Pregunta iii

Sea d tal que $(a^2 - 3a + 2 : 3a^3 - 5a^2) = d$

Usando el algoritmo de Euclides, $d = (a^2 - 3a + 2 : 6a - 8)$

Luego $(d|a^2 - 3a + 2) \wedge (d|6a - 8) \implies d|6a^2 - 18a + 12 - 6a^2 + 8a \implies d| - 10a + 12 \implies d| - 30a + 36 + 30a - 40 \implies d|4$

Por lo tanto $d \in Div_+(4) \iff d \in \{1, 2, 4\}$

Pero $\forall a : (a^2 - 3a + 2 \equiv 0(2)) \wedge (3a^3 - 5a^2 \equiv 0(2))$. Luego $d \neq 1$

Así $d \in \{2, 4\}$

a = 1 $\implies (0 : -2) = 2$ a = 2 $\implies (0 : 4) = 4$

4.21. Ejercicio 21

Por enunciado se que $(a : b) = 1 \implies 1 = s.a + t.b\ s, t \in \mathbb{Z}$

Sea $d = (7a - 3b : 2a - b)$

Se que $(d|7a - 3b) \wedge (d|2a - b) \implies d|7a - 3b - 6a + 3b \implies d|a$

De igual manera $(d|7a - 3b) \wedge (d|2a - b) \implies d|14a - 6b - 14a + 7b \implies d|b$

Luego $(d|a \wedge d|b) \implies (d|s.a \wedge d|t.b) \implies d|s.a + t.b \implies d|1$

Pero $d|1 \iff d = 1$

Por lo tanto $d = 1 \implies 7a - 3b \perp 2a - b$ como se quería probar.