Ejercicio 18 de la Práctica 4

Pablo L. De Nápoli

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Álgebra I - Primer cuatrimestre de 2020

Enunciado del ejercicio

Enunciado

18. En cada uno de los siguientes casos calcular el máximo común divisor entre a y b y escribirlo como combinación lineal entera de a y b:

$$\text{iv)} \quad a = n^2 + 1, b = n + 2 \quad (n \in \mathbb{N})$$

Hagamos un programita para ver que sucede

Salida del programa

```
for n in range(0,30):
        a=n**2+1
        b=n+2
        s,t,mcd= Euclides_extendido(a,b)
        print(n,"&",a,"&",b,"&",s,"&",t,"&",mcd,"\\\\")
```

Acá usamos la función Euclides_extendido que programamos en la clase 13 que calculaba el $mcd(a, b)$ y los coeficientes de la combinación lineal s, t tales que

$$s \cdot a + t \cdot b = mcd(a, b)$$

Salida del programa ¿Ven alguna regularidad en la tabla?

n	a	b	s	t	mcd
0	1	2	1	0	1
1	2	3	-1	1	1
2	5	4	1	-1	1
3	10	5	0	1	5
4	17	6	-1	3	1
5	26	7	3	-11	1
6	37	8	-3	14	1
7	50	9	2	-11	1
8	65	10	1	-6	5
9	82	11	-2	15	1
10	101	12	5	-42	1
11	122	13	-5	47	1
12	145	14	3	-31	1
13	170	15	1	-11	5
14	197	16	-3	37	1

n	a	b	s	t	mcd
15	226	17	7	-93	1
16	257	18	-7	100	1
17	290	19	4	-61	1
18	325	20	1	-16	5
19	362	21	-4	69	1
20	401	22	9	-164	1
21	442	23	-9	173	1
22	485	24	5	-101	1
23	530	25	1	-21	5
24	577	26	-5	111	1
25	626	27	11	-255	1
26	677	28	-11	266	1
27	730	29	6	-151	1
28	785	30	1	-26	5
29	842	31	-6	163	1

Cosas que conjeturamos mirando la tabla

$mcd(a, b) = (a : b)$ depende de la clase de n módulo 5.

Conjetura

$$(a : b) = \begin{cases} 5 & \text{si} \quad n \equiv 3 \pmod 5 \\ 1 & \text{sino} \end{cases}$$

Hacemos el algoritmo de Euclides con polinomios

Salida del programa

```
sage: var("n"); a=n**2+1; b=n+2
n
sage: Euclides_matricial_con_polinomios(a,b)
paso  0
[      1       0 n^2 + 1]
[      0       1   n + 2]
paso  1
[      1 -n + 2       5]
[      0       1  n + 2]
paso  2
[             1         -n + 2                5]
[ -1/5*n - 2/5 1/5*n^2 + 1/5                0]
(1, -n + 2, 5)
```

O sea que si tomamos $s = 1$ y $t = -n+2 = 2-n$ tenemos $s \cdot a + t \cdot b = 5$.

Demostramos nuestra conjetura (1)

Recordamos que

$$a = n^2 + 1, b = n + 2$$

Recién vimos que

$$1 \cdot a + (-n + 2) \cdot b = 5$$

Eso está bien porque

$$(-n + 2) \cdot b = (-n + 2)(n + 2) = (2 + n)(2 - n) = 4 - n^2$$

Luego:

$$1 \cdot a + (-n + 2) \cdot b = 1 + 4 - n^2 = 5$$

Ahora si $d|a$ y $d|b$, concluimos que $d|5$.
Por lo tanto

$$(a : b) = 1 \vee (a : b) = 5$$

Demostración de nuestra conjetura (2)

Miremos que pasa con los valores de a y b módulo 5. Basta hacer una tabla de restos:

n mód 5	a mód 5	b mód 5
0	1	2
1	2	3
2	$5 \equiv 0$	4
3	$10 \equiv 0$	$5 \equiv 0$
4	$17 \equiv 2$	$6 \equiv 1$

Vemos que sólo cuando $n \equiv 3 \pmod 5$, a y b resultan divisibles por 5 y en ese caso $(a : b) = 5$.
Si no, al menos uno de ellos no es divisible por 5 y resulta $(a : b) = 1$.

Continuamos...

Cuando $n \equiv 3 \pmod 5$, entonces la identidad

$$1 \cdot a + (-n + 2) \cdot b = 5$$

nos proporciona la escritura de $(a : b)$ como combinación lineal de a y b pero esto no funciona en otros casos.
¿Qué hacemos?
Lo anterior sugiere mirar tablas separadas según el resto de n módulo 5

Caso $n \equiv 0 \pmod 5$

Escribimos $n = 5q$. Recordamos que

$$a = n^2 + 1 = 25q^2 + 1, b = n + 2 = 5q + 2$$

n	q	a	b	s	t	mcd
0	0	1	2	1	0	1
5	1	26	7	3	-11	1
10	2	101	12	5	-42	1
15	3	226	17	7	-93	1
20	4	401	22	9	-164	1
25	5	626	27	11	-255	1

Notamos que nos va a servir $s = s(q) = 2q + 1$. Queremos buscar t tal que: $s \cdot a + t \cdot b = 1$. Despejando:

$$t = t(q) = \frac{1 - s \cdot a}{b} = -\frac{50q^3 + 25q^2 + 2q}{5q + 2} =$$

$$= -\frac{(10q + 1)(5q + 2)q}{5q + 2} = -(10q + 1)q$$

Caso $n \equiv 1 \pmod 5$

Escribimos $n = 5q + 1$. Recordamos que

$$a = n^2 + 1 = 25\,q^2 + 10\,q + 2, b = n + 2 = 5q + 3$$

n	q	a	b	s	t	mcd
1	0	2	3	-1	1	1
6	1	37	8	-3	14	1
11	2	122	13	-5	47	1
16	3	257	18	-7	100	1
21	4	442	23	-9	173	1
26	5	677	28	-11	266	1

Notamos que nos va a servir $s = s(q) = -(2q + 1)$. De nuevo

$$t = t(q) = \frac{1 - s \cdot a}{b} = \frac{\big(25\,q^2 + 10\,q + 2\big)(2\,q + 1) + 1}{5\,q + 3}$$

$$= 10\,q^2 + 3\,q + 1$$

Tarea para ustedes ...

Les queda pensar de modo similar los casos

$$n \equiv 2 \pmod 5$$

y

$$n \equiv 4 \pmod 5$$