Ejercicio 1

David García Curbelo

Dado tu número $n = 45352581$:

Apartado I.*Mientras n sea múltiplo de 2, 3, 5, 7 u 11 le sumas 1. De forma que tu nuevo n no tenga esos divisores primos.*

- Vemos que el número 45352581 es impar, luego no es múltiplo de 2.
- Pero, como la suma de sus dígitos es 33 (múltiplo de 3), actualizamos el valor de n añadiéndole una unidad, obteniendo 45352582 .
- Repetimos el proceso. Ahora 45352582 es múltiplo de 2, luego sumamos 1 y actualizamos su valor a 45352583 .
- Vemos que la suma de los dígitos de 45352583 es 34 el cual no es múltiplo de 3.
- Como 45352583 no acaba ni en 5 ni en 0, dicho valor no es múltiplo de 5.
- Como 45352583 módulo 7 es congruente con 3, 45352583 no es múltiplo de 7.
- Como 45352583 módulo 11 es congruente con 1, 45352583 no es múltiplo de 11.

Hemos conseguido así el número buscado, $n = 45352583$.

Apartado II. ***Calcula*** $a^{n-1} \pmod n$***, para cada uno de esas cinco bases usando sucesivamente el algoritmo izda-drcha y de drcha-izda.***

Para ambos procesos necesitaremos saber la representación de $n-1$ en base 2, para el que tenemos que $45352582_{10} = 10101101000000011010000110_2$. Como dicho número tiene 26 cifras, cada proceso constará de 26 iteraciones, siendo la última el resultado de la operación $a^{n-1} \pmod n$ para los distintos valores de a.

izda-drcha:

Base 2

Iteración	Acumulado
0	1
1	2
2	4
3	32
4	1024
5	2097152
6	4901941
7	2574340
8	24431701
9	37951484
10	6243980
11	28969616
12	32744959
13	41853729
14	1936709
15	1726249
16	42935389
17	16426326
18	36409185
19	16353216
20	45284451
21	16005958
22	27376886
23	2964308
24	27220062
25	10671452
26	5401134
	$2^{n-1} \pmod n \equiv 5401134$

Base 3

Iteración	Acumulado
0	1
1	3
2	9
3	243
4	59049
5	29259113
6	11292172
7	7525116
8	44218304
9	26775297
10	40650583
11	9371079
12	8109681
13	11498886
14	11966488
15	45258948
16	43394118
17	34167664
18	33986041
19	1181461
20	33647530
21	17298295
22	18877819
23	24620948
24	16028215
25	26671429
26	19036530
	$3^{n-1} \pmod n \equiv 19036530$

	Iteración	Acumulado
Base 5	0	1
	1	5
	2	25
	3	3125
	4	9765625
	5	9835959
	6	23733320
	7	14353170
	8	33185227
	9	24638670
	10	7540295
	11	9771990
	12	20245114
	13	14642594
	14	43749178
	15	5721504
	16	23832084
	17	36544685
	18	27160596
	19	37821484
	20	10726414
	21	37082453
	22	44314341
	23	6257820
	24	32829606
	25	11061821
	26	29804810
		$5^{n-1} \pmod{n} \equiv 29804810$

	Iteración	Acumulado
Base 7	0	1
	1	7
	2	49
	3	16807
	4	10359751
	5	15063881
	6	14246235
	7	44415909
	8	41896404
	9	28559169
	10	20398933
	11	33094120
	12	27187659
	13	22911122
	14	7960948
	15	41170261
	16	44361304
	17	38890192
	18	24907161
	19	34522948
	20	30941719
	21	31520605
	22	25095178
	23	41152615
	24	42116794
	25	44647582
	26	7452904
		$7^{n-1} \pmod{n} \equiv 7452904$

	Iteración	Acumulado
	0	1
	1	11
	2	121
	3	161051
	4	41099708
	5	18758252
	6	39784534
	7	7869852
	8	32351398
	9	11165071
	10	24998844
	11	25231382
	12	39831069
Base 11	13	22097604
	14	7087930
	15	17450229
	16	30945672
	17	37816540
	18	33735176
	19	42375724
	20	21550596
	21	5175263
	22	16407855
	23	10991810
	24	44127982
	25	28686620
	26	2015230
		$11^{n-1} \pmod{n} \equiv 2015230$

drcha-izda:

	Iteración	Exponente	Acumulado
	0	45352582	1
	1	22676291	1
	2	11338145	4
	3	5669072	64
	4	2834536	64
	5	1417268	64
	6	708634	64
	7	354317	64
	8	177158	3644558
	9	88579	3644558
	10	44289	4282517
	11	22144	31320796
	12	11072	31320796
Base 2	13	5536	31320796
	14	2768	31320796
	15	1384	31320796
	16	692	31320796
	17	346	31320796
	18	173	31320796
	19	86	32659444
	20	43	32659444
	21	21	15341136
	22	10	13749273
	23	5	13749273
	24	2	25094767
	25	1	25094767
	26	0	5401134
			$2^{n-1} \pmod{n} \equiv 5401134$

	Iteración	Exponente	Acumulado
	0	45352582	1
	1	22676291	1
	2	11338145	9
	3	5669072	729
	4	2834536	729
	5	1417268	729
	6	708634	729
	7	354317	729
	8	177158	24311052
	9	88579	24311052
	10	44289	35459567
	11	22144	35739659
	12	11072	35739659
Base 3	13	5536	35739659
	14	2768	35739659
	15	1384	35739659
	16	692	35739659
	17	346	35739659
	18	173	35739659
	19	86	41990270
	20	43	41990270
	21	21	21307220
	22	10	37476107
	23	5	37476107
	24	2	45273497
	25	1	45273497
	26	0	19036530
			$3^{n-1} \pmod{n} \equiv 19036530$

	Iteración	Exponente	Acumulado
Base 5	0	45352582	1
	1	22676291	1
	2	11338145	25
	3	5669072	15625
	4	2834536	15625
	5	1417268	15625
	6	708634	15625
	7	354317	15625
	8	177158	41450728
	9	88579	41450728
	10	44289	5511674
	11	22144	3328245
	12	11072	3328245
	13	5536	3328245
	14	2768	3328245
	15	1384	3328245
	16	692	3328245
	17	346	3328245
	18	173	3328245
	19	86	24581849
	20	43	24581849
	21	21	25673283
	22	10	21813943
	23	5	21813943
	24	2	43254326
	25	1	43254326
	26	0	29804810
			$5^{n-1} \pmod{n} \equiv 29804810$

	Iteración	Exponente	Acumulado
	0	45352582	1
	1	22676291	1
	2	11338145	49
	3	5669072	117649
	4	2834536	117649
	5	1417268	117649
	6	708634	117649
	7	354317	117649
	8	177158	28491703
	9	88579	28491703
	10	44289	4829743
	11	22144	17486073
	12	11072	17486073
Base 7	13	5536	17486073
	14	2768	17486073
	15	1384	17486073
	16	692	17486073
	17	346	17486073
	18	173	17486073
	19	86	24761580
	20	43	24761580
	21	21	18994483
	22	10	22336683
	23	5	22336683
	24	2	32942235
	25	1	32942235
	26	0	27704450
			$7^{n-1} \pmod{n} \equiv 27704450$

	Iteración	Exponente	Acumulado
	0	45352582	1
	1	22676291	1
	2	11338145	121
	3	5669072	1771561
	4	2834536	1771561
	5	1417268	1771561
	6	708634	1771561
	7	354317	1771561
	8	177158	23163409
	9	88579	23163409
	10	44289	18945097
	11	22144	43014292
	12	11072	43014292
Base 11	13	5536	43014292
	14	2768	43014292
	15	1384	43014292
	16	692	43014292
	17	346	43014292
	18	173	43014292
	19	86	11213684
	20	43	11213684
	21	21	37482594
	22	10	37985641
	23	5	37985641
	24	2	18608191
	25	1	18608191
	26	0	26386779
			$11^{n-1} \pmod{n} \equiv 26386779$

Apartado III.*¿Es n un posible primo de Fermat para alguna de ellas? ¿Es n un pseudoprimo para alguna de ellas?*

- Para que n sea un posible primo de Fermat para alguna base, n debe pasar el test para dicha base. Como hemos visto en el apartado anterior, ninguna de las cinco bases mencionadas cumplen $1 \equiv a^{n-1} \pmod{n}$, Luego n no es primo de Fermat para ninguna de dichas bases.
- Para que n sea un pseudoprimo para alguna base, n debe de pasar el test para dicha base y además ser compuesto. Como no se cumple para ninguna base, no tenemos la condición de que n sea un pseudoprimo para ninguna de las bases.