

## Álgebra I

### Práctica 3 - Números enteros (Parte 1)

#### Divisibilidad y algoritmo de división

1. Decidir cuáles de las siguientes afirmaciones son verdaderas  $\forall a, b, c \in \mathbb{Z}$

- |   |  |
|---|--|
| i) $a \cdot b \mid c \Rightarrow a \mid c$ y $b \mid c$ ,   | vi) $a \mid c$ y $b \mid c \Rightarrow a \cdot b \mid c$ ,         |
| ii) $4 \mid a^2 \Rightarrow 2 \mid a$ ,                     | vii) $a \mid b \Rightarrow a \leq b$ ,                             |
| iii) $2 \mid a \cdot b \Rightarrow 2 \mid a$ ó $2 \mid b$ , | viii) $a \mid b \Rightarrow  a  \leq  b $ ,                        |
| iv) $9 \mid a \cdot b \Rightarrow 9 \mid a$ ó $9 \mid b$ ,  | ix) $a \mid b + a^2 \Rightarrow a \mid b$ ,                        |
| v) $a \mid b + c \Rightarrow a \mid b$ ó $a \mid c$ ,       | x) $a \mid b \Rightarrow a^n \mid b^n, \forall n \in \mathbb{N}$ . |

2. Hallar todos los  $n \in \mathbb{N}$  tales que

- |                            |                              |
|----------------------------|------------------------------|
| i) $3n - 1 \mid n + 7$ ,   | iii) $2n + 1 \mid n^2 + 5$ , |
| ii) $3n - 2 \mid 5n - 8$ , | iv) $n - 2 \mid n^3 - 8$ .   |

3. Sean  $a, b \in \mathbb{Z}$ .

- i) Probar que  $a - b \mid a^n - b^n$  para todo  $n \in \mathbb{N}$  y  $a \neq b \in \mathbb{Z}$ . (c.f. Ejercicio 5 Práctica 2.)
- ii) Probar que si  $n$  es un número natural par y  $a \neq -b$ , entonces  $a + b \mid a^n - b^n$ .
- iii) Probar que si  $n$  es un número natural impar y  $a \neq -b$ , entonces  $a + b \mid a^n + b^n$ .

4. Sea  $a$  un entero impar. Probar que  $2^{n+2} \mid a^{2^n} - 1$  para todo  $n \in \mathbb{N}$ .

5. Sea  $n \in \mathbb{N}$ . Probar que

- i) si  $n \neq 1$  y  $n \mid (n - 1)! + 1$  entonces  $n$  es primo
- ii) si  $n$  es compuesto, entonces  $2^n - 1$  es compuesto.

(Los primos de la forma  $2^p - 1$  para  $p$  primo se llaman *primos de Mersenne*, por Marin Mersenne, monje y filósofo francés, 1588-1648. Se conjetura que existen infinitos primos de Mersenne, pero aún no se sabe. Hasta hoy, abril 2015, se conocen 48 primos de Mersenne. El más grande producido hasta ahora es  $2^{57885161} - 1$ , que tiene 17425170 dígitos, y es el número primo más grande conocido a la fecha.)

- iii) si  $2^n + 1$  es primo, entonces  $n$  es una potencia de 2.

(Los números de la forma  $\mathcal{F}_n = 2^{2^n} + 1$  se llaman *números de Fermat*, por Pierre de Fermat, juez y matemático francés, 1601-1665. Fermat conjeturó que cualquiera sea  $n \in \mathbb{N} \cup \{0\}$ ,  $\mathcal{F}_n$  era primo, pero esto resultó falso: los primeros  $\mathcal{F}_0 = 3$ ,  $\mathcal{F}_1 = 5$ ,  $\mathcal{F}_2 = 17$ ,  $\mathcal{F}_3 = 257$ ,  $\mathcal{F}_4 = 65537$ , son todos primos, pero  $\mathcal{F}_5 = 4294967297 = 641 \times 6700417$ . Hasta ahora no se conocen más primos de Fermat que los 5 primeros mencionados...)

6. Probar que

- i) El producto de  $n$  enteros consecutivos es divisible por  $n!$
- ii)  $\binom{2n}{n}$  es divisible por 2,
- iii)  $2^n \cdot \prod_{i=1}^n (2i - 1)$  es divisible por  $n!$
- iv)  $\binom{2n}{n}$  es divisible por  $n + 1$  (sugerencia: probar que  $(2n + 1)\binom{2n}{n} = (n + 1)\binom{2n+1}{n}$  y observar que  $\binom{2n}{n} = (2n + 2)\binom{2n}{n} - (2n + 1)\binom{2n}{n}$ ).

7. Probar que las siguientes afirmaciones son verdaderas para todo  $n \in \mathbb{N}$

i)  $99 \mid 10^{2n} + 197$ ,

iii)  $56 \mid 13^{2n} + 28n^2 - 84n - 1$ ,

ii)  $9 \mid 7 \cdot 5^{2n} + 2^{4n+1}$ ,

iv)  $256 \mid 7^{2n} + 208n - 1$ .

8. Calcular el cociente y el resto de la división de  $a$  por  $b$  en los casos

i)  $a = 133$ ,  $b = -14$ ,

iv)  $a = b^2 - 6$ ,  $b \neq 0$ ,

ii)  $a = 13$ ,  $b = 111$ ,

v)  $a = n^2 + 5$ ,  $b = n + 2$  ( $n \in \mathbb{N}$ ),

iii)  $a = 3b + 7$ ,  $b \neq 0$ ,

vi)  $a = n + 3$ ,  $b = n^2 + 1$  ( $n \in \mathbb{N}$ ).

9. Sabiendo que el resto de la división de un entero  $a$  por 18 es 5, calcular el resto de

i) la división de  $a^2 - 3a + 11$  por 18,

iv) la división de  $a^2 + 7$  por 36,

ii) la división de  $a$  por 3,

v) la división de  $7a^2 + 12$  por 28,

iii) la división de  $4a + 1$  por 9,

vi) la división de  $1 - 3a$  por 27.

10. i) Determinar todos los  $a, b \in \mathbb{Z}$  coprimos tales que  $\frac{b+4}{a} + \frac{5}{b} \in \mathbb{Z}$ .

ii) Determinar todos los  $a, b \in \mathbb{Z}$  coprimos tales que  $\frac{9a}{b} + \frac{7a^2}{b^2} \in \mathbb{Z}$ .

iii) Determinar todos los  $a \in \mathbb{Z}$  tales que  $\frac{2a+3}{a+1} + \frac{a+2}{4} \in \mathbb{Z}$ .

iv) Determinar todos los  $k \in \mathbb{N}$  tales que  $\binom{12k}{2}$  divide a  $12k \binom{3k+6}{2}$ .

#### Máximo común divisor y ecuaciones diofánticas

11. 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  $b$ :

i)  $a = 2532$ ,  $b = 63$ ,

iii)  $a = 131$ ,  $b = 23$ ,

ii)  $a = 5335$ ,  $b = 110$ ,

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

12. Determinar, cuando existan, todos los  $(a, b) \in \mathbb{Z}^2$  que satisfacen

i)  $5a + 8b = 3$ ,

iii)  $24a + 14b = 7$ ,

v)  $39a - 24b = 6$ .

ii)  $7a + 11b = 10$

iv)  $20a + 16b = 36$

vi)  $1555a - 300b = 11$

13. Determinar todos los  $(a, b) \in \mathbb{Z}^2$  que satisfacen simultáneamente  $4 \mid a$ ,  $8 \mid b$  y  $33a + 9b = 120$ .

14. Si se sabe que cada unidad de un cierto producto A cuesta 39 pesos y que cada unidad de un cierto producto B cuesta 48 pesos, ¿cuántas unidades de cada producto se pueden comprar con 135 pesos?

15. Sean  $a, b \in \mathbb{Z}$ . Sabiendo que el resto de dividir  $a$  por  $b$  es 27 y que el resto de dividir  $b$  por 27 es 21, calcular  $(a : b)$ .

16. i) ¿Cuántas veces hay que aplicar el algoritmo de división para calcular mediante el algoritmo de Euclides el máximo común divisor  $(F_{n+1} : F_n)$  entre dos números de Fibonacci consecutivos?

ii) ¿Existen números  $b \leq a \in \mathbb{N}$  con  $b \leq F_n$  que requieran más aplicaciones del algoritmo de división que los del inciso (i) para calcular su máximo común divisor  $(a : b)$ ?

iii) Dados  $b \leq a \in \mathbb{N}$ , ¿cuál es la cantidad máxima de veces que hay que aplicar el algoritmo de división para calcular  $(a : b)$  mediante el algoritmo de Euclides, en términos de  $b$ ?

17. Sea  $a \in \mathbb{Z}$ .

- i) Probar que  $(5a + 8 : 7a + 3) = 1$  o 41. Exhibir un valor de  $a$  para el cual da 1, y verificar que efectivamente para  $a = 23$  da 41.
- ii) Probar que  $(2a^2 + 3a - 1 : 5a + 6) = 1$  o 43. Exhibir un valor de  $a$  para el cual da 1, y verificar que efectivamente para  $a = 16$  da 43.

18. Sean  $a, b \in \mathbb{Z}$  coprimos. Probar que  $7a - 3b$  y  $2a - b$  son coprimos.

19. Sean  $a, b \in \mathbb{Z}$  con  $(a : b) = 2$ . Probar que los valores posibles para  $(7a + 3b : 4a - 5b)$  son 2 y 94. Exhibir valores de  $a$  y  $b$  para los cuales da 2 y para los cuales da 94.

20. Sea  $a, b \in \mathbb{Z}$  no ambos nulos. Probar que:

- i)  $(ca : cb) = |c|(a : b)$ ,  $\forall c \in \mathbb{Z}$  con  $c \neq 0$ ,
- ii)  $(a : b) = 1$  y  $(a : c) = 1 \Leftrightarrow (a : bc) = 1$ ,
- iii)  $(a : b) = d$  y  $(a : c) = 1 \Rightarrow (a : bc) = d$ ,
- iv) si  $(a : b) = 1$  entonces  $(a : b^2) = 1$ ,
- v)  $(a : b) = 1 \Leftrightarrow (a^n : b^m) = 1, \forall n, m \in \mathbb{N}$ ,
- vi)  $(a : b) = d \Leftrightarrow (a^n : b^n) = d^n, \forall n \in \mathbb{N}$ .

21. Sea  $n \in \mathbb{N}$ . Probar que

- i)  $(2^n + 7^n : 2^n - 7^n) = 1$ ,
- ii)  $(2^n + 5^{n+1} : 2^{n+1} + 5^n) = 3$  ó 9, y dar un ejemplo para cada caso.
- iii)  $(3^n + 5^{n+1} : 3^{n+1} + 5^n) = 2$  ó 14, y dar un ejemplo para cada caso.

22. Sean  $a, b \in \mathbb{Z}$ . Probar que si  $(a : b) = 1$  entonces  $(a^2 \cdot b^3 : a + b) = 1$ .

23. Sean  $a, b \in \mathbb{Z}$  tales que  $(a : b) = 5$ .

- i) Calcular los posibles valores de  $(\bar{a}b : 5a - 10b)$  y dar un ejemplo para cada uno de ellos.
- ii) Para cada  $n \in \mathbb{N}$ , calcular  $(a^{n-1}b : a^n + b^n)$ .

24. Sea  $n \in \mathbb{N}$  coprimo con 10. Probar que existe un múltiplo de  $n$  de la forma 111...1.

25. Sea  $a \in \mathbb{Z}$ ,  $a > 1$  y sean  $n, m \in \mathbb{N}$ .

- i) Probar que si  $r$  es el resto de la división de  $n$  por  $m$ , entonces el resto de la división de  $a^n - 1$  por  $a^m - 1$  es  $a^r - 1$ .
- ii) Probar que  $(a^n - 1 : a^m - 1) = a^{(n:m)} - 1$ .

26. i) Dados  $a, b \in \mathbb{Z}$  coprimos, probar que existe una matriz de  $2 \times 2$  con coordenadas enteras y determinante 1 tal que su primera fila sea  $a, b$ .

ii) Dados  $a_1, a_2, \dots, a_n \in \mathbb{Z}$ , probar que son las coordenadas de la primera fila de una matriz entera cuyo determinante es exactamente  $(a_1 : a_2 : \dots : a_n)$ .

27. *El algoritmo de Euclides binario* es una variante del algoritmo de Euclides que sólo utiliza divisiones por 2, lo que resulta ventajoso si se opera con números escritos en el sistema binario (como sucede en una computadora), ya que en ese caso la división por 2 es muy simple (cf. Ej. 60).

i) Sean  $a, b \in \mathbb{Z}$  no ambos nulos. Probar las siguientes igualdades

$$(a : b) = \begin{cases} a & \text{si } b = 0 \\ 2\left(\frac{a}{2} : \frac{b}{2}\right) & \text{si } a \text{ es par y } b \text{ es par} \\ \left(\frac{a}{2} : b\right) & \text{si } a \text{ es par y } b \text{ es impar} \\ \left(a : \frac{b}{2}\right) & \text{si } a \text{ es impar y } b \text{ es par} \\ \left(\frac{a-b}{2} : b\right) & \text{si } a \text{ es impar y } b \text{ es impar} \end{cases}$$

- ii) Diseñar un algoritmo para calcular el máximo común divisor entre dos números positivos en base a las identidades anteriores, y probar que siempre termina (la correctitud está dada por el inciso (i)). Por ejemplo, para calcular el máximo común divisor entre 60 y 42, el algoritmo funcionaría de la manera siguiente:

$$\begin{aligned}(60 : 42) &= 2(30 : 21) = 2(21 : 15) = 2(3 : 15) = 2(15 : 3) \\ &= 2(6 : 3) = 2(3 : 3) = 2(0 : 3) = 2(3 : 0) = 2 \cdot 3 = 6.\end{aligned}$$

(Si  $a$  y  $b$  están escritos en base 2, y  $n$  es la cantidad de bits del mayor de los dos números, este algoritmo requiere a lo sumo del orden de  $n^2$  operaciones bit, ya que en cada paso se divide un número por 2, y las restas y las divisiones por 2 requieren recorrer todos los bits.)

### Primos y factorización

28. i) Probar que un número natural  $n$  es compuesto si y sólo si es divisible por algún primo positivo  $p \leq \sqrt{n}$ .  
 ii) Determinar cuáles de los siguientes enteros son primos: 91, 209, 307, 791, 1001, 3001.  
 iii) Hallar todos los primos menores o iguales que 100.

29. Probar que 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503 y 4973 son números primos.

30. Probar que existen infinitos primos congruentes a 3 módulo 4.

Sugerencia: probar primero que si  $a \neq \pm 1$  satisface  $a \equiv 3 \pmod{4}$ , entonces existe  $p$  primo,  $p \equiv 3 \pmod{4}$  tal que  $p \mid a$ . Luego probar que si existieran sólo finitos primos congruentes a 3 módulo 4, digamos  $p_1, p_2, \dots, p_n$ , entonces  $a = -1 + 4 \prod_{i=1}^n p_i$  sería un entero distinto de 1 y  $-1$  que no es divisible por ningún primo congruente a 3 módulo 4.

31. Otra prueba algebraica de la infinitud de los números primos, utilizando los números de Fermat  $\mathcal{F}_n = 2^{2^n} + 1$  (cf. Ej. 5 item (ii)) (Demostración de George Pólya, matemático húngaro, 1887–1985):

- i) (cf. Ej. 3(ii)) Probar que para todo  $n \in \mathbb{N} \cup \{0\}$  par y todo  $a \in \mathbb{Z}$ ,  $a \neq -1$ , se tiene

$$\frac{a^n - 1}{a + 1} = a^{n-1} - a^{n-2} + a^{n-3} - \dots + a - 1.$$

- ii) Probar que  $\mathcal{F}_n \mid \mathcal{F}_m - 2$  si  $m > n$  y deducir que  $\mathcal{F}_n$  y  $\mathcal{F}_m$  son coprimos si  $n \neq m$ .  
 iii) Concluir que existen infinitos primos distintos.

32. Decidir si existen enteros  $a$  y  $b$  no nulos que satisfagan

$$\text{i) } a^2 = 8b^2, \quad \text{ii) } a^2 = 3b^3, \quad \text{iii) } 7a^2 = 11b^2.$$

33. Sea  $n \in \mathbb{N}$ ,  $n \geq 2$ . Probar que si  $p$  es un primo positivo entonces  $\sqrt[n]{p} \notin \mathbb{Q}$ .

34. i) Calcular las máximas potencias de 3 y de 9 que dividen a  $77!$   
 ii) Calcular la máxima potencia de 20 que divide a  $81!$   
 iii) Calcular la máxima potencia de 24 que divide a  $81!$   
 iv) Determinar en cuántos ceros termina el desarrollo decimal de  $81!$   
 v) Determinar en cuántos ceros termina el desarrollo en base 16 de  $20!$

35. Sea  $p$  un número primo y  $n \in \mathbb{N}$ . Sea  $p^\alpha$  la mayor potencia de  $p$  que divide a  $n!$ . Probar que

$$\alpha = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

(la suma sólo tiene un número finito de términos no nulos).

36. Sea  $n \in \mathbb{N}$  y  $p$  un primo impar tal que  $\frac{2n}{3} < p \leq n$ . Probar que  $p$  no divide a  $\binom{2n}{n}$ .
37. Sea  $p^k$  potencia de un número primo que divide a  $\binom{2n}{n}$ . Probar que  $p^k \leq 2n$ .
38. Sean  $p$  y  $q$  primos positivos distintos y sea  $n \in \mathbb{N}$ . Probar que si  $pq \mid a^n$  entonces  $pq \mid a$ .
39. Sean  $a, b \in \mathbb{Z}$ . Probar que si  $ab$  es un cuadrado en  $\mathbb{Z}$  y  $(a : b) = 1$ , entonces tanto  $a$  como  $b$  son cuadrados en  $\mathbb{Z}$ .
40. Sea  $p$  primo positivo. Probar que si  $0 < k < p$ , entonces  $p$  divide a  $\binom{p}{k}$ .
41. Sea  $p$  un primo positivo. Probar que  $n^p - n$  es múltiplo de  $p$ , para todo  $n \in \mathbb{N}$ .
42. i) Sea  $m \in \mathbb{N}$ . Probar que  $\prod_{m+1 < p \leq 2m+1} p$  divide a  $\binom{2m+1}{m}$ .
- ii) Probar que  $\prod_{p \leq n} p \leq 4^n$ , donde el producto se extiende a todos los primos menores o iguales a  $n \in \mathbb{N}$ . Sugerencia: inducción y el ejercicio 37 (iii) de la práctica 2.
43. *Ternas Pitagóricas, S. VI A.C.* Son las ternas  $(a, b, c)$  de números naturales que satisfacen

$$a^2 + b^2 = c^2,$$

o sea que se corresponden con las longitudes de los catetos e hipotenusa de triángulos rectángulos con lados enteros.

- i) Probar que si  $(a, b, c)$  es una terna pitagórica, entonces  $(ka, kb, kc)$  es una terna pitagórica,  $\forall k \in \mathbb{N}$ .
- ii) Probar que si existe  $k \in \mathbb{N}$  que divide a dos de los términos, entonces divide también al tercero.
- iii) Probar que existen infinitas ternas pitagóricas *primitivas* (aquellas donde  $a$ ,  $b$  y  $c$  son coprimos) que satisfacen que  $c = b + 1$ , como por ejemplo  $(3, 4, 5)$ ,  $(5, 12, 13)$  y  $(7, 24, 25)$ .  
(Sug: Probar que el conjunto  $\{1^2 - 0^2, 2^2 - 1^2, 3^2 - 2^2, \dots\}$  coincide con el conjunto de los números naturales impares, y considerar en él los cuadrados de los impares.)
- iv) Sean  $m > n \in \mathbb{N}$ . Probar que la siguiente es una terna pitagórica

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

Probar que es primitiva si y solo si  $m$  y  $n$  son coprimos, uno de los dos es impar y el otro par.

- v) Caracterización de todas las ternas pitagóricas *primitivas*:
- (a) Probar que  $c$  tiene que ser impar obligatoriamente (sug: tomar congruencia módulo 4), y que entre  $a$  y  $b$  hay uno que es par y el otro que es impar.
- (b) Sean  $a$  el impar y  $b$  el par. Probar que  $(c - a : c + a) = 2$  y de  $b^2 = c^2 - a^2 = (c - a)(c + a)$ , deducir que  $c - a = 2n^2$  y  $c + a = 2m^2$  para algún  $n < m \in \mathbb{N}$ . Concluir.

44. Determinar cuántos divisores positivos tienen  $9000$ ,  $15^4 \cdot 42^3 \cdot 56^5$  y  $10^n \cdot 11^{n+1}$ . ¿Y cuántos divisores en total?
45. Hallar la suma de los divisores positivos de  $2^4 \cdot 5^{123}$  y de  $10^n \cdot 11^{n+1}$ .
46. Hallar el menor número natural  $n$  tal que  $6552n$  sea un cuadrado.
47. Hallar todos los  $n \in \mathbb{N}$  tales que
- i)  $(n : 945) = 63$ ,  $(n : 1176) = 84$  y  $n \leq 2800$ ,
- ii)  $(n : 1260) = 70$  y  $n$  tiene 30 divisores positivos.

48. Hallar el menor número natural  $n$  tal que  $(n : 3150) = 45$  y  $n$  tenga exactamente 12 divisores positivos.

49. Hallar todos los  $n \in \mathbb{N}$  tales que

i)  $[n : 130] = 260$ .

ii)  $[n : 420] = 7560$ .

50. Hallar todos los  $a, b \in \mathbb{Z}$  tales que

i)  $(a : b) = 10$  y  $[a : b] = 1500$ .

ii)  $3 \mid a$ ,  $(a : b) = 20$  y  $[a : b] = 9000$ .

51. Sea  $n \geq 2$  un entero.

i) Probar que

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$$

no es entero.

Sugerencia: considerar la mayor potencia de 2 menor o igual a  $n$ .

ii) Probar que

$$1 + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{2n-1}$$

no es entero.

52. Sea  $h : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  definida por  $h(x, y) = 2^{x-1}(2y-1)$ . Probar que es biyectiva.

53. Sea  $h : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  definida por  $h(x, y, z) = 2^{x-1}3^{y-1}5^{z-1}$ . Probar que es inyectiva pero no sobreyectiva.

\* 54. *Postulado de Bertrand*. Sea  $n$  un número natural y  $N = \prod_{n < p \leq 2n} p$  el producto de todos los primos entre  $n$  y  $2n$ .

i) Probar que

$$\binom{2n}{n} \leq 2^{4n/3} (2n)^{\sqrt{2n}} N.$$

Sugerencia: Ejercicios 36, 37 y 42.

ii) Probar que para todo  $n \in \mathbb{N}$  existe al menos un número primo  $p$  tal que  $n < p \leq 2n$ .

Sugerencia: Ejercicios 12 (viii) y 14 (vi) de la Práctica 2 y 29 de esta Práctica.

\* 55. Sea  $n \geq 1$ . Probar que para toda elección de  $n+1$  números enteros  $1 \leq a_1 < a_2 < \dots < a_{n+1} \leq 2n$  existen dos tales que su suma  $a_i + a_j = p$  es un número primo.

### Sistemas de numeración

56. i) Hallar el desarrollo en base 2 de

(a) 1365,

(b) 2800,

(c)  $3 \cdot 2^{13}$ ,

(d)  $13 \cdot 2^n + 5 \cdot 2^{n-1}$ .

ii) Hallar el desarrollo en base 7 de 8575

iii) Hallar el desarrollo en base 16 de 4074, 4064 y 16448250.

57. Sea  $a \in \mathbb{N}_0$ . Probar que si el desarrollo en base 10 de  $a$  termina en  $k$  ceros entonces el desarrollo en base 5 de  $a$  termina en por lo menos  $k$  ceros.

58. i) ¿Cuáles son los números naturales más chico y más grande que se pueden escribir con exactamente  $n$  "dígitos" en base  $d > 1$ ?

- ii) Probar que  $a \in \mathbb{N}_0$  tiene a lo sumo  $\lceil \log_2(a) \rceil + 1$  bits cuando se escribe su desarrollo binario. (Para  $x \in \mathbb{R}_{\geq 0}$ ,  $\lceil x \rceil$  es la *parte entera de  $x$* , es decir el mayor número natural (o cero) que es menor o igual que  $x$ .)
- 59.** i) Sea  $k = 2^{n+1} - 1$ . Calcular la cantidad de cuentas que hay que hacer para calcular  $a^k$  adaptando el algoritmo “dividir y conquistar” del Ejercicio 53 (ii) de la Práctica 2 (sugerencia: escribir  $k$  en base 2).
- ii) ¿Cuál es la máxima cantidad de cuentas que hay que hacer para calcular  $a^k$  para  $k \in \mathbb{N}$  cualquiera, siguiendo ese mismo algoritmo?
- iii) ¿Cuál es la máxima cantidad de cuentas que hay que hacer para calcular el  $n$ -ésimo número de Fibonacci  $F_n$  de esta forma (con el modelo del Ejercicio 55 de la Práctica 2)?
- 60.** Sea  $a = (a_d a_{d-1} \dots a_1 a_0)_2$  un número escrito en base 2 (o sea escrito en bits). Determinar simplemente cómo son las escrituras en base 2 del número  $2a$  y del número  $a/2$  cuando  $a$  es par, o sea las operaciones “multiplicar por 2” y “dividir por 2” cuando se puede. Esas operaciones se llaman *shift* en inglés, o sea corrimiento, y son operaciones que una computadora hace en forma sencilla (comparar con el Ej. 38 de la Práctica 1).
- 61.** Enunciar y demostrar criterios de divisibilidad por 8, 9 y 11.
- \* **62.** Sea  $f : \mathbb{N} \rightarrow \mathbb{N}$  una función definida recursivamente por  $f(1) = 1$ ,  $f(3) = 3$ , y para  $n \neq 1, 3$

$$f(n) = \begin{cases} f\left(\frac{n}{2}\right) & \text{si } n \text{ es par} \\ 2f\left(\frac{n+1}{2}\right) - f\left(\frac{n-1}{4}\right) & \text{si } 4|n - 1 \\ 3f\left(\frac{n-1}{2}\right) - 2f\left(\frac{n-3}{4}\right) & \text{si } 4|n - 3. \end{cases}$$

Determine el número de enteros positivos  $n \leq 2047$  para los que  $f(n) = n$ .

- \* **63.** i) Escribir a  $10^n$  en base 2 y en base 5 para  $n = 1, 2, 3, 4, 5$  y 6. ¿Qué fenómeno observa?
- ii) Hallar en función de  $n \in \mathbb{N}$  la cantidad de cifras del desarrollo de  $10^n$  en base 2 y en base 5.
- iii) Con la ayuda del ejercicio 51 de la Práctica 2, probar el fenómeno observado en el ítem (i).
- \* **64.** Probar que
- i)  $2^n$  no divide a  $n!$ .
- ii) si  $2^{n-1} | n!$  entonces  $n$  es potencia de 2.