FCEyN - UBA - Verano 2015

Álgebra I
Práctica 3 - Números enteros (Parte 1)

Divisibilidad

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

i) $a \cdot b \mid c \Rightarrow a \mid c$ y $b \mid c$,
ii) $4 \mid a^2 \Rightarrow 2 \mid a$,
iii) $2 \mid a \cdot b \Rightarrow 2 \mid a$ ó $2 \mid b$,
iv) $9 \mid a \cdot b \Rightarrow 9 \mid a$ ó $9 \mid b$,
v) $a \mid b + c \Rightarrow a \mid b$ ó $a \mid c$,
vi) $a \mid c$ y $b \mid c \Rightarrow a \cdot b \mid c$,
vii) $a \mid b \Rightarrow a \leq b$,
viii) $a \mid b \Rightarrow |a| \leq |b|$,
ix) $a \mid b + a^2 \Rightarrow a \mid b$,
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) $3n - 1 \mid n + 7$,
ii) $3n - 2 \mid 5n - 8$,
iii) $2n + 1 \mid n^2 + 5$,
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 es compuesto, entonces $2^n - 1$ es compuesto.
ii) si $2^n + 1$ es primo, entonces n es una potencia de 2.

Notas históricas:

- 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 (febrero de 2014), 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.
- 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) $\binom{2n}{n}$ 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) $99 \mid 10^{2n} + 197$,
ii) $9 \mid 7 \cdot 5^{2n} + 2^{4n+1}$,
iii) $56 \mid 13^{2n} + 28n^2 - 84n - 1$,
iv) $256 \mid 7^{2n} + 208n - 1$.

Algoritmo de División

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

i) $a = 133, \quad b = -14$,
ii) $a = 13, \quad b = 111$,
iii) $a = 3b + 7, \quad b \neq 0$,
iv) $a = b^2 - 6, \quad b \neq 0$,
v) $a = n^2 + 5, \quad b = n + 2$ $(n \in \mathbb{N})$,
vi) $a = n + 3, \quad b = n^2 + 1$ $(n \in \mathbb{N})$.

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

i) $a^2 - 3a + 11$ por 18,
ii) a por 3,
iii) $4a + 1$ por 9,
iv) $a^2 + 7$ por 36,
v) $7a^2 + 12$ por 28,
vi) $1 - 3a$ por 27.

10.
i) Suponiendo que $a \equiv 22\ (14)$, hallar el resto de dividir a a por 14, por 2 y por 7.
ii) Suponiendo que $a \equiv 13\ (5)$, hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.
iii) Hallar, para cada $n \in \mathbb{N}$, el resto de la división de $\sum_{i=1}^{n} (-1)^i \cdot i!$ por 36.

11.
i) Hallar todos los $a \in \mathbb{Z}$ tales que $a^2 \equiv 3\ (11)$.
ii) Probar que no existe ningún entero a tal que $a^3 \equiv -3\ (13)$.
iii) Probar que $a^2 \equiv -1\ (5) \Leftrightarrow a \equiv 2\ (5)$ ó $a \equiv 3\ (5)$.
iv) Probar que $a^7 \equiv a\ (7)$ para todo $a \in \mathbb{Z}$.
v) Probar que $7 \mid a^2 + b^2 \Leftrightarrow 7 \mid a$ y $7 \mid b$.
vi) Probar que $5 \mid a^2 + b^2 + 1 \Rightarrow 5 \mid a$ ó $5 \mid b$.

12.
i) Probar que $2^{5n} \equiv 1\ (31)$ para todo $n \in \mathbb{N}$.
ii) Hallar el resto de la división de 2^{51833} por 31.
iii) Sea $k \in \mathbb{N}$. Sabiendo que $2^k \equiv 39\ (31)$, hallar el resto de la división de k por 5.
iv) Hallar el resto de la división de $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ por 31.

Sistemas de numeración

13.
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 16 de 2800.

14. 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.

15.
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 $[\log_2(a)] + 1$ bits (dígitos en la base 2) cuando se escribe su desarrollo binario. (Para $x \in \mathbb{R}_{\geq 0}$, $[x]$ es la *parte entera de* x, es decir el mayor número natural o cero que es menor o igual que x.)

16. 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 37 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? (Expresarla como función de k.)

17. Sea $a = (a_d a_{d-1} \dots a_1 a_0)_2$ un número escrito en base 2 (o sea escrito en el sistema binario). Determinar 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. ¿Por qué resultan sencillas de realizar para una computadora? Comparar con la multiplicación y división por 10 en el sistema decimal.

18. Enunciar y demostrar criterios de divisibilidad por 8, 9 y 11.

Máximo común divisor

19. 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) $a = 2532$, $b = 63$,

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

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

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

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

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

i) Probar que $(5a + 8 : 7a + 3) = 1$ o 41. Comprobar que si $a = 23$ entonces el resultado es 41, y exhibir un valor de a para el cual el resultado sea 1.

ii) Probar que $(2a^2 + 3a - 1 : 5a + 6) = 1$ o 43. Comprobar que si $a = 16$ entonces el resultado es 43, y exhibir un valor de a para el cual el resultado sea 1.

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

23. 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.

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

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

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

25. *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. 17).

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

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

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 y da el resultado correcto. Por ejemplo, para calcular el máximo común divisor entre 60 y 42, el algoritmo funcionaría de la manera siguiente:

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

Primos y factorización

26. i) Probar que un número natural n es compuesto si y sólo si es divisible por algún primo positivo $p \le \sqrt{n}$.

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.

27. i) Si $a \neq \pm 1$ satisface $a \equiv 3 \pmod 4$, entonces existe un primo p tal que $p \equiv 3 \pmod 4$ y $p \mid a$.

ii) Probar que si existieran sólo finitos primos congruentes a 3 módulo 4, digamos $p_1, p_2, \ldots, p_n$, 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. Concluir que existen infinitos primos congruentes a 3 módulo 4.

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

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

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

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.

29. Sea $p \in \mathbb{N}$ un número primo. Probar que si $0 < k < p$, entonces p divide a $\binom{p}{k}$.

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

i) $a^2 = 8b^2$, ii) $a^2 = 3b^3$, iii) $7a^2 = 11b^2$.

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

32. Sean p y q primos positivos distintos y sea $n \in \mathbb{N}$. Probar que si $p\,q \mid a^n$ entonces $p\,q \mid a$.

33. 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 $\mathbb{Z}$.

34. Determinar cuántos divisores positivos, y cuántos divisores enteros, tienen 9000, $15^4 \cdot 42^3 \cdot 56^5$ y $10^n \cdot 11^{n+1}$.

35. Hallar la suma de los divisores positivos de $2^4 \cdot 5^{123}$ y de $10^n \cdot 11^{n+1}$.

36. Hallar el menor número natural n tal que $6552\,n$ sea un cuadrado.

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

i) $(n:945) = 63$, $(n:1176) = 84$ y $n \le 2800$,

ii) $(n:1260) = 70$ y n tiene 30 divisores positivos.

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

39. 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.

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

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

i) Calcular los posibles valores de $(ab : 5a - 10b)$ y dar un ejemplo para cada uno de ellos.

ii) Para cada $n \in \mathbb{N}$, calcular $(a^{n-1}b : a^n + b^n)$.

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

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

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

43. 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 $[a : b] = 9000$.