FCEyN - UBA - Segundo Cuatrimestre 2013

Álgebra I
Práctica 3 - Números enteros (Parte 1)

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

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

5. 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 9 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 $a + b \mid a^n + b^n$.

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

i) 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: el más grande producido hasta Febrero 2013 es $2^{257885161} - 1$.)
ii) 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 (Mayo 2013) no se conocen más primos de Fermat que los 5 primeros mencionados...)

7. 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 $\binom{2n}{n} = (2n+2)\binom{2n}{n} - (2n+1)\binom{2n}{n}$).

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

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

10. 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.

11. Sea a un entero. Probar que si el desarrollo en base 10 de a termina en n ceros entonces el desarrollo en base 5 de a termina en por lo menos n ceros.

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

ii) Probar que $a \in \mathbb{N}$ tiene a lo sumo $\lfloor \log_2(a) \rfloor + 1$ bits cuando se escribe su desarrollo binario. (Para $x \in \mathbb{R}_{\geq 0}$, $\lfloor x \rfloor$ es la *parte entera de* x, es decir el mayor número natural (o cero) que es menor o igual que x.)

13. i) Sea $n = 2^{k+1} - 1$. Calcular la cantidad de cuentas que hay que hacer para calcular a^n adaptando el algoritmo "dividir y conquistar" del Ejercicio 23 de la Práctica 2 (sugerencia: escribir n en base 2).

ii) ¿Cuál es la máxima cantidad de cuentas que hay que hacer para calcular a^n para $n \in \mathbb{N}$ 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 24 de la Práctica 2).

14. 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. 30 de la Práctica 1).

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

16. 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 $(a : b)$.

17. 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?

18. 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 $(a^n - 1 : a^m - 1) = a^{(n:m)} - 1$.

19. Probar que si $(a : b) = 1$ entonces $(7a - 3b : 2a - b) = 1$, $\forall\, a, b \in \mathbb{Z}$.

20. *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. 14).

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.)

iii) Para pensar: ¿Cómo podría adaptarse este algoritmo de Euclides binario para que también proporcione los coeficientes que permiten escribir al máximo común divisor como una combinación lineal de los números en cuestión?

21. 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 ?

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

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

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

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

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

26. i) *Criba de Eratóstenes (∼ 200 A.C.).* 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.

27. 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 $p_1, p_2, \ldots, p_n$, 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.

28. Otra prueba algebraica de la infinitud de los números primos, utilizando los números de Fermat $\mathcal{F}_n = 2^{2^n} + 1$ (cf. Ej. 6) (Demostración de George Pólya, matemática húngaro, 1887–1985):

i) (cf. Ej. 4(ii)) Probar que para todo $n \in \mathbb{N} \cup \{0\}$ *par* y todo $a \in \mathbb{Z}$, $a \neq 1$, se tiene

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

ii) Probar que $\mathcal{F}_n | \mathcal{F}_m - 2$ 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. Sean $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$. Probar que $a \mid b \Leftrightarrow a^n \mid b^n$ (comparar con Ej.1(x)).

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

31. Sean $a, b \in \mathbb{Z}$. Probar que si ab es un cuadrado en $\mathbb{Z}$ y a y b son coprimos, entonces tanto a como b son cuadrados en $\mathbb{Z}$.

32. Sea p primo positivo. Probar que si $0 < k < p$, entonces p divide a $\binom{p}{k}$.

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

i) $(c\,a : c\,b) = |c|\,(a : b),\ \forall c \in \mathbb{Z}$ 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) $(a : b) = 1 \ \Leftrightarrow\ (a^n : b^m) = 1, \forall\, n, m \in \mathbb{N}$,

v) $(a : b) = d \ \Leftrightarrow\ (a^n : b^n) = d^n, \forall\, n \in \mathbb{N}$.

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

i) $(2^n + 7^n : 2^n - 7^n) = 1$,

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

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

36. 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,

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

37. Hallar todos los $a, b \in \mathbb{Z}$ tales que $(a : b) = 10$ y $[\,a : b\,] = 1500$.