FCEyN - UBA - 1er cuatrimestre 2016

Álgebra I
Práctica 4 - Números enteros (Parte 1)

Divisibilidad y números primos

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

4. Hallar todos los $n \in \mathbb{Z}$ tales que $n^2 + n + 1 \mid n^3 - 22$.

5. 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) $256 \mid 7^{2n} + 208n - 1$.

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

i) Probar que $a - b \mid a^n - b^n$ para todo $n \in \mathbb{N}$. (c.f. Ejercicio 7 Práctica 3.)
ii) Probar que si n es un número natural impar, entonces $a + b \mid a^n + b^n$.
iii) Probar que si n es un número natural par, entonces $a + b \mid a^n - b^n$.

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

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

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

9.
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.

10. 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 2016, se conocen 49 primos de Mersenne. El más grande producido hasta ahora es $2^{74207281} - 1$, que tiene 22338618 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...)

∗ **11**. *Criba de Eratóstenes*

El siguiente algoritmo computa la Criba de Eratóstenes para los números hasta un N dado.

```
Para k = 2 Hasta N Hacer
   C_k := Verdadero
Fin Para
Para k = 2 Hasta N Hacer
   Si C_k es Verdadero Entonces
      Para i desde 2 hasta ⌊N/k⌋ Hacer
         C_{i×k} = Falso
      Fin Para
   Fin Si
Fin Para
```

"Corra" el algoritmo *a mano* para $N = 20$. Compruebe que cuando termina el algoritmo, C_k es *Verdadero* si y sólo si k es primo. Dado N, ¿cuántas operaciones realiza el algoritmo? Teniendo en cuenta el item i) del ejercicio 9, ¿qué optimizaciones podemos hacerle al algoritmo?

Algoritmo de división y sistemas de numeración

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

13. 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.

14. Sean $a_1, a_2, a_3, \ldots, a_n$ números enteros. Probar que existen índices i, j con $1 \leq i \leq j \leq n$ tales que $\sum_{k=i}^{j} a_k$ es divisible por n. (Sugerencia: considere los restos en la división por n de los n números a_1, $a_1 + a_2$, $a_1 + a_2 + a_3$, …, $a_1 + a_2 + \ldots + a_n$.)

15. 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.

16. 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.

17. 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 $\lfloor \log_2(a) \rfloor + 1$ 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.)

18. 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 Ejercicio 37 de la Práctica 1).

∗ **19**. Sea $f : \mathbb{N} \to \mathbb{N}$ una función definida recursivamente por $f(1) = 1$, y para $n > 1$

$$f(n) = \begin{cases} f(\frac{n}{2}) & \text{si } n \text{ es par,} \\ f(\frac{n-1}{2}) + 1 & \text{si } n \text{ es impar.} \end{cases}$$

¿Cuántos enteros positivos $n \leq 2047$ cumplen que $f(n) = 9$?

Congruencia y tablas de restos

20. i) Si $a \equiv 22\ (14)$, hallar el resto de dividir a a por 14, por 2 y por 7.

ii) Si $a \equiv 13\ (5)$, hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.

21. Hallar, para cada $n \in \mathbb{N}$, el resto de la división de $\sum_{i=1}^{n} (-1)^i \cdot i!$ por 36.

22. 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.

23. Sea a un entero impar que no es divisible por 5.

i) Probar que $a^4 \equiv 1\ (10)$.

ii) Probar que a y a^{45321} tienen el mismo resto en la división por 10.

24. 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 $3 \mid a^2 + b^2 \Leftrightarrow 3 \mid a$ y $3 \mid b$.

v) Probar que $7 \mid a^2 + b^2 \Leftrightarrow 7 \mid a$ y $7 \mid b$.

vi) Probar que $5 \mid a^2 + b^2 \Leftrightarrow a \equiv 2b\ (5)$ ó $a \equiv 3b\ (5)$.

vii) Probar que $5 \mid a^2 + b^2 + 1 \Rightarrow 5 \mid a$ ó $5 \mid b$.

viii) Probar que cualesquiera sean $a, b, c \in \mathbb{Z}$, $a^2 + b^2 + c^2 + 1$ no es divisible por 8.

25. Demostrar que ninguna de las siguientes ecuaciones tiene soluciones enteras:

i) $x^3 - 2 = 7y$, ii) $15x^2 - 7y^2 = 9$, iii) $3x^2 + 2 = y^3$.

∗ **26**. Probar que la ecuación $x^2 + y^2 = 3$ no tiene soluciones con $(x, y) \in \mathbb{Q}^2$.

27. Probar que para todo $n \in \mathbb{N}$, el número $19 \cdot 14^n + 1$ no es primo.

28. Sea p un número primo. Probar que si $p \mid a - b$, entonces $p^{n+1} \mid a^{p^n} - b^{p^n}$ para todo $n \in \mathbb{N}_0$.

Máximo común divisor

29. 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.

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

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

32. Sean $a, b \in \mathbb{Z}$. Sabiendo que el resto de dividir a a por b es 27 y que $b \equiv 48 \pmod{27}$, calcular $(a : b)$.

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

34. Verificar que la siguiente función computa correctamente el Máximo Común Divisor:

```
Función mcd(a,b)
   Si b=0 Entonces
      Devolver a
   Fin Si
   Devolver mcd(b,a % b)
Fin Función
```

Aquí a % b denota al resto de dividir a por b. La función está implementada de manera iterativa. ¿Cuántas iteraciones ocurren si llamamos a la función en el par (F_{n+1}, F_n), es decir dos términos consecutivos de la sucesión de Fibonacci? ¿Qué podemos decir en general si la llamamos en el par (a, b)?

35. Sean 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) $(a : b) = 1 \Leftrightarrow (a^n : b^m) = 1$, $\forall\, n, m \in \mathbb{N}$.

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

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

37. 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.

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

39. 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 $(a^{n-1}b : a^n + b^n)$.

40. 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.

∗ **41**. Sea $n \in \mathbb{N}$ coprimo con 10. Probar que existe un múltiplo de n de la forma $111 \ldots 11$.

Ecuaciones diofánticas y de congruencia

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

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

ii) $7a + 11b = 10$,

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

iv) $20a + 16b = 36$,

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

vi) $1555a - 300b = 11$.

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

44. Determinar todos los $b \in \mathbb{Z}$ para los cuales existe $a \equiv 4\ (5)$ tal que $6a + 21b = 15$.

45. Para una multitudinaria fiesta se espera la presencia de exactamente 5000 invitados. Los organizadores disponen de dos tipos de mesas con las que deben asegurar que no falte ni sobre ningún lugar para que se sienten todos los invitados: mesas medianas, para 8 personas cada una, y mesas grandes, para 14 personas cada una. Además, los organizadores son supersticiosos, y quieren que la cantidad total de mesas utilizadas sea un múltiplo de 13. ¿De cuántas maneras distintas pueden elegir la cantidad de mesas de cada tipo?

46. Hallar, cuando existan, todas las soluciones de las siguientes ecuaciones de congruencia:

i) $17X \equiv 3\ (11)$,

ii) $56X \equiv 28\ (35)$,

iii) $56X \equiv 2\ (884)$,

iv) $33X \equiv 27\ (45)$.

47. Hallar el resto de la división de un entero a por 18, sabiendo que el resto de la división de $7a$ por 18 es 5.

48. Hallar todos los $n \in \mathbb{N}$ para los cuales $n^3 + 4n + 5 \equiv n - 1\ (n^2 + 1)$.

49. Hallar todos los $(a, b) \in \mathbb{Z}^2$ tales que $b \equiv 2a \pmod 5$ y $28a + 10b = 26$.

50. Hallar todos los $a \in \mathbb{Z}$ para los cuales $(7a + 1 : 5a + 4) \neq 1$.

51. Describir los valores de $(5a + 8 : 7a + 3)$ en función de los valores de $a \in \mathbb{Z}$.