Algebra I
Segundo Cuatrimestre — 2006

Práctica 4: Números enteros, I

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

   a) $ab \mid c \implies a \mid c \wedge b \mid c$;
   b) $4 \mid a^2 \implies 2 \mid a$;
   c) $2 \mid ab \implies 2 \mid a \vee 2 \mid b$;
   d) $9 \mid ab \implies 9 \mid a \vee 9 \mid b$;
   e) $a \mid b + c \implies a \mid b \vee a \mid c$;
   f) $a \mid c \wedge b \mid c \implies ab \mid c$;
   g) $a \mid b \implies a \leq b$;
   h) $a \mid b + a^2 \implies a \mid b$.

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

   a) $3n - 1 \mid n + 7$;
   b) $3n - 2 \mid 5n - 8$;
   c) $2n + 1 \mid n^2 + 5$;
   d) $n - 2 \mid n^3 - 8$.

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

   a) $99 \mid 10^{2n} + 197$;
   b) $9 \mid 7 \cdot 5^{2n} + 2^{4n+1}$;
   c) $56 \mid 13^{2n} + 28n^2 - 84n - 1$;
   d) $256 \mid 7^{2n} + 208n - 1$.

4. *a*) Probar que $a - b \mid a^n - b^n$ para todo $n \in \mathbb{N}$.
   b) Probar que si n es un número natural par entonces $a + b \mid a^n - b^n$.
   c) Probar que si n es un número natural impar entonces $a + b \mid a^n + b^n$.

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

   a) El producto de n enteros consecutivos es divisible por $n!$.
   b) $\binom{2n}{n}$ es divisible por 2.
   c) $2^n \prod_{i=1}^{n}(2i - 1)$ es divisible por $n!$.
   d) $\binom{2n}{n}$ es divisible por $n + 1$.

   Sugerencia: probar que

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

6. Hallar todos los primos positivos menores o iguales que 100

7. *a*) Probar que un número natural n es compuesto si y sólo si es divisible por algún primo positivo $p \leq \sqrt{n}$.

b) Determinar cuáles de los siguientes enteros son primos: 91, 209, 307, 791, 1001, 3001.

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

   a) si $n \mid (n-1)! + 1$ entonces n es primo;

   b) si $2^n - 1$ es primo entonces n es primo;

   c) si $2^n + 1$ es primo entonces n es una potencia de 2.

9. Probar que existen infinitos primos.

   Sugerencia: probar que si existieran finitos primos $p_1, p_2, \dots, p_n$, entonces $a = 1 + \prod_{i=1}^{n} p_i$ sería un entero distinto de 1 y -1 que no es divisible por ningún primo. Esta idea es debida a Euclides.

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

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

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

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

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

    e) $a = n^2 + 5$, $b = n + 2$, $\forall n \in \mathbb{N}$;

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

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

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

    b) la división de a por 3;

    c) la división de $4a + 1$ por 9;

    d) la división de $a^2 + 7$ por 36;

    e) la división de $7a^2 + 12$ por 28;

    f) la división de $1 - 3a$ por 27.

12. Hallar todos los $n \in \mathbb{N}$ para los cuales el resto de la división de $n^3 + 4n + 5$ por $n^2 + 1$ sea $n - 1$.

13. Sean $a_1, a_2, \dots, a_n$ enteros. Probar que existen r, s tales que $\sum_{j=0}^{s} a_{r+j}$ es divisible por n

    Sugerencia: Considere los n números a_1, $a_1 + a_2$, $a_1 + a_2 + a_3$, ..., $a_1 + a_2 + \cdots a_n$ y pruebe que si ninguno de ellos es divisible por n entonces necesariamente dos de ellos tienen el mismo resto en la división por n.

14. *a*) Hallar el desarrollo en base 2 de:

    i) 1365;

    ii) 2800;

    iii) $3 \cdot 2^{13}$;

    iv) $13 \cdot 2^n + 5 \cdot 2^{n-1}, \forall n \in \mathbb{N}$.

    b) Hallar el desarrollo en base 7 de 8575.

    c) Hallar el desarrollo en base 16 de 2800.

    d) 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.

15. *a*) Sea $a \in \mathbb{Z}$ tal que $a \equiv 22 \pmod{14}$. Hallar el resto de dividir a a por 2, por 7 y por 14.

    b) Sea $a \in \mathbb{Z}$ tal que $a \equiv 13 \pmod{5}$. Hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.

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

16. *a*) Hallar todos los $a \in \mathbb{Z}$ tales que $a^2 \equiv 3 \pmod{11}$.

    b) Probar que no existe ningún entero a tal que $a^3 \equiv -3 \pmod{13}$.

    c) Probar que $a^2 \equiv -1 \pmod{5} \iff a \equiv 2 \pmod{5}$ ó $a \equiv 3 \pmod{5}$.

    d) Probar que $a^7 \equiv a \pmod{7}$, $\forall a \in \mathbb{Z}$.

    e) Probar que $3 \mid a^2 + b^2 \iff 3 \mid a$ y $3 \mid b$.

    f) Probar que $7 \mid a^2 + b^2 \iff 7 \mid a$ y $7 \mid b$.

    g) Probar que $5 \mid a^2 + b^2 \iff a \equiv 2b \pmod{5}$ ó $a \equiv 3b \pmod{5}$.

    h) Probar que $5 \mid a^2 + b^2 + 1 \implies 5 \mid a$ ó $5 \mid b$.

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

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

    a) Probar que $a^4 \equiv 1 \pmod{10}$.

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

18. *a*) Probar que $2^{5n} \equiv 1 \pmod{31}$ para todo $n \in \mathbb{N}$.

    b) Hallar el resto de la división de 2^{51833} por 31.

    c) Sea $k \in \mathbb{N}$. Sabiendo que $2^k \equiv 39 \pmod{31}$, hallar el resto de la división de k por 5.

    d) Hallar el resto de la división de $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ por 31.

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

    b) Hallar el resto de la división de 5^{2267} por 32.

20. Sean $a, b, c \in \mathbb{Z}$ tales que $a^2 + b^2 = c^2$. Probar que:

    a) $3 \mid a$ ó $3 \mid b$;

    b) $5 \mid a$ ó $5 \mid b$ ó $5 \mid c$;

    c) $4 \mid a$ ó $4 \mid b$;

21. Enunciar y demostrar los criterios de divisibilidad por 2, 3, 4, 5, 8, 9 y 11.

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

    Sugerencia: probar primero que un número congruente a 3 módulo 4 distinto de 1 y -1 necesariamente es divisible por un primo congruente a 3 módulo 4. Luego probar que si existieran 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.

23. 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:

    a) $a = 2532$, $b = 63$;
    b) $a = 5335$, $b = 110$;
    c) $a = 131$, $b = 23$;
    d) $a = n^2 + 1$, $b = n + 2$, para todo $n \in \mathbb{N}$.

24. 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 $(a : b)$.

25. Sea $a \in \mathbb{Z}$, $a > 1$ y sean $n, m \in \mathbb{N}$. Probar que $(a^n - 1 : a^m - 1) = a^{(n:m)} - 1$.

    Sugerencia: 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 $a^r - 1$.

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

    a) Probar que $(5a + 8 : 7a + 3) = 1$ ó 41.
    b) Probar que $(2a^2 + 3a - 1 : 5a + 6) = 1$ ó 43.

27. a) Determinar todos los $a, b \in \mathbb{Z}$ coprimos tales que $\frac{b+4}{a} + \frac{5}{b} \in \mathbb{Z}$.
    b) Determinar todos los $a, b \in \mathbb{Z}$ coprimos tales que $\frac{9a}{b} + \frac{7a^2}{b^2} \in \mathbb{Z}$.
    c) Determinar todos los $a \in \mathbb{Z}$ tales que $\frac{2a+3}{a+1} + \frac{a+2}{4} \in \mathbb{Z}$.

28. Sean $a, b, c \in \mathbb{Z}$. Mostrar que, si a y b son coprimos, es $(a : bc) = (a : c)$.

    Sugerencia: probar que $(a : bc)$ y b son coprimos.

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

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

31. a) Sean $a, b, c \in \mathbb{Z}$, $c > 0$. Probar que $(ca : cb) = c(a : b)$
    b) Sean $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Mostrar que:
        i) Si $(a : b) = 1$ entonces $(a^n : b^n) = 1$.
        ii) Si $(a : b) = d$ entonces $(a^n : b^n) = d^n$.
        iii) Si $a^n \mid b^n$ entonces $a \mid b$.

32. Sean $a, b \in \mathbb{Z}$. Probar que:

    a) si $(a : b) = 1$ entonces $(7a - 3b : 2a - b) = 1$;
    b) si $(a : b) = 1$ entonces $(2a - 3b : 5a + 2b) = 1$ ó 19;
    c) si $(a : b) = 2$ entonces $(5a - 3b : 4a + b) = 2$ ó 34;
    d) si $(a : b) = 3$ entonces $(a.b^2 : 9a + 9b) = 27$.

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

    a) $(2^n + 7^n : 2^n - 7^n) = 1$;

b) $(2^n + 5^{n+1} : 2^{n+1} + 5^n) = 3$ ó 9;

c) $(3^n + 5^{n+1} : 3^{n+1} + 5^n) = 2$ ó 14.

34. Determinar, cuando existan, todos los $a, b \in \mathbb{Z}$ que satisfacen las siguientes condiciones:

a) $5a + 8b = 3$;

b) $7a + 11b = 10$;

c) $24a + 14b = 7$;

d) $20a + 16b = 36$;

e) $39a - 24b = 6$;

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

35. 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?

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

a) $17X \equiv 3 \pmod{11}$;

b) $56X \equiv 2 \pmod{884}$;

c) $56X \equiv 28 \pmod{35}$;

d) $33X \equiv 27 \pmod{45}$.

37. 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.

38. *a*) Hallar todos los $a \in \mathbb{Z}$ tales que $(7a + 1 : 5a + 4) \neq 1$.

b) Hallar todos los $a \in \mathbb{Z}$ tales que $(2a^2 + 3a - 1 : 5a + 6) \neq 1$.

Johann Carl Friedrich Gauss
1777–1855, Alemania