TEORÍA DE NÚMEROS Curso 2004/2005 Lista 1

Repaso de congruencias y divisibilidad

1. Sea $\mathcal{H} = \{5, 9, 13, 17, 21, \dots\}$. Decimos que $n \in \mathcal{H}$ es $\mathcal{H}$-primo si no tiene divisores propios en $\mathcal{H}$. Demostrar que la factorización en $\mathcal{H}$-primos no es única.

2. Demostrar que hay infinitos primos de la forma $6n + 5$.

3. Si contamos con los dedos de una mano de la forma habitual (comenzando por el índice y acabando en el pulgar), ¿en qué dedo terminará la cuenta hasta 7^{7^7}? ¿y si somos B. Simpson, que sólo tiene cuatro dedos?

4. Sea $F(n) = 2^n + 1$ con $n \in \mathbb{Z}, n > 0$.

a) Demostrar que si $F(n) = r \cdot s$, con $r, s > 1$, entonces las máximas potencias de 2 que dividen a $r - 1$ y a $s - 1$ coinciden.

b) Los números $F(n)$ se llaman *primos de Fermat* si son primos y *números de Fermat* si $n = 2^k$, $k \in \mathbb{N}$, en cuyo caso se suelen denotar por $F_k = 2^{2^k} + 1$. Demostrar que los primos de Fermat son números de Fermat. *Indicación*: Probar que si a es impar $2^b + 1 | 2^{ab} + 1$.

c) Demostrar que $\prod_{k=0}^{n-1} F_k = F_n - 2$.

d) Demostrar que dos números de Fermat distintos son primos entre sí y deducir de ello que hay infinitos números primos.

5. He comprado bolígrafos a 1'01 euros y rotuladores a 1'40 euros. Si me he gastado en total 29'93 euros, ¿cuántos he comprado de cada?

6. Se llaman *primos de Mersenne* a los primos de la forma $M_n = 2^n - 1$.

a) Demostrar que si M_n es primo, entonces n es primo.

b) Comprobar que el recíproco no se cumple.

7. Hallar todas las soluciones de $x^4 + 3x^2 + 2 \equiv 0$ módulo 30 y módulo 45.

8. ¿En qué cifra acaba 13^{2004}?

9. Hallar en cuántos ceros termina 131!

10. Demostrar la desigualdad $(n!)^{1/n} \leq \prod_{p|n} p^{1/(p-1)}$, y deducir que hay infinitos números primos a partir de que la sucesión $a_n = (n!)^{1/n}$ diverge.

11. Demostrar que hay infinitos números que no son suma de dos ni de tres cuadrados. *Indicación*: ¿Qué ocurre en $\mathbb{Z}_8$?

12. Sean $x, y, z \in \mathbb{Z}$ tales que $x^2 + y^2 = z^2$. Demostrar que al menos uno de los números x, y, z es divisible por 3, al menos uno es divisible por 4 y al menos uno es divisible por 5.

13. En diferentes contextos se busca un "principio local-global" que permita transformar congruencias para muchos módulos en igualdades. A continuación veremos algunos impedimentos para que tal principio funcione sin hipótesis añadidas.

a) Sea n un entero y p un número primo. Demostrar que $x^2 + y^2 = n \mod p$ tiene al menos una solución. *Indicación*: ¿cuántos cuadrados hay módulo p?

b) Sea $f(x_1, \ldots, .x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ un polinomio en n variables con coeficientes enteros. Decidir si es verdadera o falsa la siguiente afirmación "Si $f(x_1, \ldots, x_n) \equiv 0\ (p)$ tiene solución para todo primo p, entonces $f(x_1, \ldots, .x_n) = 0$ tiene soluciones enteras".

c) Hacer lo mismo con la siguiente afirmación "Si $f(x_1, \ldots, x_n) \equiv 0\ (p)$ tiene solución para todo primo p, entonces $f(x_1, \ldots, .x_n) \equiv 0\ (m)$ tiene soluciones para todo entero m".

14. Demostrar que si un entero $n > 1$ cumple $(n-1)! \equiv -1\ (n)$, entonces es primo.

15. Calcular la probabilidad de que un número natural no sea divisible ni por 2 ni por 3 ni por 5, tratando de dar un sentido riguroso a esta probabilidad. Concluir que menos del 30 % de los números son primos (Nota: En realidad la proporción es nula, en cierto modo, por el teorema de los números primos).

16. Un número n se llama *perfecto para el producto* si $\prod_{d|n} d = n^2$, es decir, si al multiplicar todos los divisores de n, excepto el propio n, obtenemos de nuevo n. Encontrar una caracterización de los números perfectos para el producto en términos de su factorización como producto de primos.

17. Aunque no lo parezca, este problema está relacionado con los números p-ádicos que se mencionan más adelante.

a) Demostrar que si $x^2 \equiv a\ (p)$ tiene solución con p primo impar, entonces también tiene solución módulo p^n, con n cualquier entero positivo.

b) Si $P \in \mathbb{Z}_p[x]$ tiene una raíz $r \in \mathbb{Z}_p$ y $P'(r) \not\equiv 0\ (p)$, entonces tiene solución módulo p^n, con n cualquier entero positivo. Nota: Éste resultado, en otro lenguaje, es lo que se llama *Lema de Hensel*.

Tres para fanáticos de la topología

18. Sea $\mathcal{B}$ la colección de todas las progresiones aritméticas no constantes $\{qn + a : n \in \mathbb{Z}\}$ y sea $\mathcal{P}$ el conjunto números primos.

a) Demostrar que $\mathcal{B}$ es base para una topología en $\mathbb{Z}$.

b) Demostrar que $\{2n : n \in \mathbb{Z}\}$ es un conjunto cerrado.

c) Demostrar que, en general, todos los elementos de $\mathcal{B}$ son cerrados.

d) Demostrar que $\mathbb{Z} \setminus \{-1, 1\}$ no es cerrado.

e) Demostrar que $\cup_{p \in \mathcal{P}} \{pn : n \in \mathbb{Z}\} = \mathbb{Z} \setminus \{-1, 1\}$.

f) Deducir de los apartados anteriores que hay infinitos primos.

19. Sea $c(n)$ la mayor potencia de 5 que divide a $n \in \mathbb{Z} \setminus \{0\}$ (p. ej. $c(75) = 5^2$, $c(12) = 5^0$, etc.). Demostrar que

$$d(n, m) = \begin{cases} 0 & \text{si } n = m \\ \frac{1}{c(n-m)} & \text{si } n \neq m \end{cases}$$

define una distancia en $\mathbb{Z}$. Demostrar que en este espacio métrico la sucesión de enteros 10, 1100, 111000, 11110000, ... es convergente. ¿Cuál es su límite?

20. Sea p un número primo. Para $x \in \mathbb{Q} \setminus \{0\}$, se define $v_p(x)$ como el único entero tal que $x = p^{v_p(x)} a/b$ con $(a, p) = (b, p) = 1$. Además se suele definir $v_p(0) = +\infty$. Se llama *valor absoluto p-ádico* en $\mathbb{Q}$ a $\|x\|_p = p^{-v_p(x)}$. (Nota: El espacio obtenido al completar $\mathbb{Q}$ dotado de esta norma con todos lo límites de sucesiones de Cauchy, es muy relevante en teoría de números y a sus elementos se les llama *números p-ádicos*).

a) Recordar la propiedad arquimediana de $\mathbb{Q}$: dados $a, b \in \mathbb{Q}$ con $0 < a < b$ existe $n \in \mathbb{Z}$ tal que $|na| > |b|$. Demostrar que si en lugar del valor absoluto usual usamos el valor absoluto p-ádico, esto ya no es cierto.

b) Demostrar que $\|x + y\|_p \leq \text{máx}\{\|x\|_p, \|y\|_p\}$.

c) La bola p-ádica de centro $a \in \mathbb{Q}$ y radio r es $B(a, r) = \{x \in \mathbb{Q} \mid \|x - a\|_p \leq r\}$. Demostrar que cualquier punto de $B(a, r)$ es un centro (p-ádico) de $B(a, r)$.

d) Sea $\mathcal{P}^+ = \{primos\} \cup \{\infty\}$ y definamos, para $x \in \mathbb{Q}$, $\|x\|_\infty = |x|$. Demostrar que, para todo $x \in \mathbb{Q} - \{0\}$, se tiene la *fórmula del producto*: $\prod_{p \in \mathcal{P}^+} \|x\|_p = 1$.

Raíces primitivas, Euler-Fermat

21. Demostrar que si un primo, p, divide a $4n^2+1$ con $n \geq 1$, entonces $4|p-1$. Utilizar el resultado para probar que hay infinitos primos de la forma $4m + 1$. *Indicación*: Sea g una raíz primitiva módulo p y α tal que $g^\alpha \equiv 2n\ (p)$. Probar que $4\alpha/(p-1)$ es un entero impar.

22. Para cada una de las ecuaciones $x^{22} \equiv 101\ (225)$, $x^{27} \equiv 76\ (225)$, $x^{37} \equiv 176\ (225)$, hallar una solución, o demostrar que no existe.

23. Probar que si m y n son coprimos entonces $m^{\phi(n)} + n^{\phi(m)} \equiv 1\ (mn)$.

24. Comprobar que 2 es una raíz primitiva módulo 29 y utilizarla para encontrar todas las soluciones de $x^7 \equiv 1\ (29)$.

25. Encontrar una raíz primitiva módulo 125.

26. Sea p un primo impar. Demostrar que si a es raíz primitiva módulo p^n entonces también lo es módulo p.

27. ¿A qué grupo sencillo es isomorfo el grupo de unidades de $\mathbb{Z}_{140}$? ¿Cuántas soluciones tiene $x^{12} \equiv 1\ (140)$?

28. Supongamos que en $\mathbb{Z}_m^*$ es cíclico. Demostrar que si $(a, m) = 1$ y $(k, \phi(m)) = 1$ entonces el polinomio $x^k - a$ tiene una sola raíz en $\mathbb{Z}_m$.

29. Sea el homomorfismo $\phi : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*$ dado por $\phi(x) = x^n$ con $n|p - 1$. Hallar el cardinal de Im ϕ.

30. En este ejercicio estudiaremos la estructura de grupo de $\mathbb{Z}_{2^e}^*$ para $e \geq 3$.

a) Demostrar por inducción que $5^{2^{e-3}} \equiv 1 + 2^{e-1}\ (2^e)$ y concluir que el orden de 5 en $\mathbb{Z}_{2^e}^*$ es 2^{e-2}.

b) Demostrar que $\{(-1)^a 5^b \mid 0 \leq a \leq 1, 0 \leq b < 2^{e-2}\}$ es un conjunto de representantes de $\mathbb{Z}_{2^e}^*$.

c) Demostrar que $\mathbb{Z}_{2^e}^* \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{e-2}}$.

31. Demostrar que el producto de todas las raíces primitivas módulo p es congruente con $(-1)^{\phi(p-1)}$. *Indicación*: Comenzar probando que la suma de los números $1 \leq n \leq p-1$ coprimos con $p - 1$ es $(p - 1)\ \phi(p - 1)/2$.

32. Se llama carácter (de Dirichlet) a cualquier homomorfismo no nulo de $\mathbb{Z}_n^*$ en $\mathbb{C} - \{0\}$, ambos grupos con el producto. Hallar todos los caracteres para $n = 10$.

Funciones aritméticas

33. Hallar una fórmula para la suma de las raíces cuadradas de los divisores de un número.

34. Demostrar que si $F(n)$ es multiplicativa, $f(n) = \sum_{d|n} F(d)\mu(n/d)$ también lo es.

35. Calcular la suma de $d^{-1}\phi(d)$ sobre todos los divisores de un millón.

36. Hallar $\sum_{d|n} |\mu(d)|$ en términos de la factorización de n.

37. ¿Para qué valores es $\sigma(n)$ impar?

38. Demostrar que si a y n son coprimos, n divide a $\sum_{d|n} a^d \mu(n/d)$. *Indicación*: Estudiar primero el caso $n = p^\alpha$.

39. Se define la función λ de Liouville como $\lambda(1) = 1$ y $\lambda(n) = (-1)^{k_1+k_2+\cdots+k_r}$ si $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ con $p_1, p_2, \dots, p_r$ primos distintos. Hallar $\sum_{d|n} \lambda(d)$.

40. Se dice que un número n es perfecto si la suma de todos sus divisores, $\sigma(n)$, es $2n$. Demostremos con Euler que, si n es un número par perfecto, entonces $n = 2^{p-1}(2^p - 1)$, donde $2^p - 1$ es un primo de Mersenne.

a) Sea $n = 2^k m$ con $k \geq 1$, m impar y n perfecto. Comprobar que existe un entero c tal que $\sigma(m) = 2^{k+1}c$.

b) Deducir que $m = (2^{k+1} - 1)c$ y que si $c > 1$ se tendría $\sigma(m) \geq 1 + 2^{k+1}c$, lo que es una contradicción.

c) Probar que $\sigma(m) = m + 1$ y que por tanto m es primo.

d) Concluir que efectivamente debe ser $n = 2^{p-1}(2^p - 1)$ con p y $2^p - 1$ primos.

e) Encontrar todos los números perfectos (pares) entre 1.000 y 33.000.000.

41. Se conjetura que no hay números perfectos impares, pero este problema clásico parece estar fuera del alcance de los métodos actuales.

a) Sea p un número primo. Demostrar que p^m no es perfecto.

b) Sean p, q dos números primos impares distintos. Demostrar que $p^m q^n$ no es perfecto.

42. Sea $(f * g)(n) = \sum_{d|n} f(d)g(n/d)$. Describir explícitamente las funciones $\mathbf{1} * \mathbf{1}$, $\mathbf{1} * id$ y $\mu * \sigma$.

43. Probar que $\sum_{n|N} (d(n))^3 = \left(\sum_{n|N} d(n)\right)^2$. *Indicación*: Tratar primero el caso p^m por inducción en m.

44. Sea la función $\Lambda(n) = \log p$ si $n = p^\alpha$, $\alpha \geq 1$, y $\Lambda(n) = 0$ en otro caso. Hallar $\sum_{d|n} \mu(d)\Lambda(n/d)$. *Indicación*: Si no se usa la función ζ, distínganse los casos $\mu(n) \neq 0$ y $\mu(n) = 0$.

45. Fijado $K \in \mathbb{N}$, sea $R_K(n) = \sum_j e^{2\pi i j K/n}$ donde j recorre los números $1 \leq j \leq n$ con $(j, n) = 1$. Demostrar que $R_K(n)$ es multiplicativa.

46. Con la notación del ejercicio anterior, hallar una fórmula para $R_1(n)$.

47. Sea $N \in \mathbb{Z}^+$, calcular el valor de $\sum_{n=1}^{N} \mu(n)[N/n]$ donde $[\,\cdot\,]$ indica la parte entera. *Indicación*: Hallar una fórmula para el cardinal de los $n \leq N$ que no son divisibles por ningún primo.

48. Sea N_n el número de polinomios mónicos irreducibles de grado n en $\mathbb{Z}_p[x]$.

a) Calcular N_2.

b) Probar la fórmula $N_n = n^{-1} \sum_{d|n} \mu(n/d)p^d$. *Indicación*: Es necesario recordar los cuerpos finitos de Álgebra II. A cada polinomio irreducible de grado n en $\mathbb{F}_p$ se le puede asociar una de sus raíces, las cuales están en $\mathbb{F}_{p^n}$, son distintas y no pertenecen a ningún subcuerpo propio de $\mathbb{F}_{p^n}$.

c) Demostrar que en $\mathbb{F}_p$ hay polinomios irreducibles de todos los grados.

49. Demostrar que $\sum_{n=1}^{\infty} \mu(n)x^n(1-x^n)^{-1} = x$.

Función ζ y distribución de primos

50. Deducir que hay infinitos primos de la igualdad . $\zeta(2) = \pi^2/6$ sabiendo que π^2 es irracional.

51. Hallar $\prod_p (p^2-1)^2/(p^4-1)$ y $\prod_p (1+p^{-2})$. Nota: $\zeta(4) = \pi^4/90$.

52. Calcular la probabilidad de que un número "escogido al azar" no sea divisible por ningún cuadrado mayor que 1.

53. Escribir $\sum_{n=1}^{\infty} d(n)n^{-s}$ en términos de la función ζ.

54. Repetir el problema anterior cambiando $d(n)$ por $\sigma(n)$ (la suma de los divisores).

55. Demostrar que $\sum_{n=1}^{\infty} d^2(n)n^{-s} = \zeta^4(s)/\zeta(2s)$. *Indicación*: Este problema es más difícil que los dos anteriores. Considérese la serie $1^2 + 2^2x + 3^2x^2 + 4^2x^3 + \ldots$ y trátese de sumarla usando cálculo infinitesimal.

56. El postulado de Bertrand también se cumple si reemplazamos el intervalo $[n, 2n)$ por $[x, 2x-6)$ para $x \geq 9$, $x \in \mathbb{R}$. Sabiendo esto, demostrar que todo número mayor que 6 se puede escribir como suma de primos distintos.

57. Demostrar que $\sum_{n=1}^{N} n^{-1}$ no es entero para ningún $N \geq 2$. *Indicación*: Encontrar un primo que divida al denominador pero no al numerador.

58. Dando por supuestas las hipótesis del teorema de Ikehara y utilizando ejercicios anteriores, deducir el comportamiento asintótico de $\sum_{n \leq x} \phi(n)/n$, $\sum_{n \leq x} \sigma(n)/n$ y $\sum_{n \leq x} d^2(n)$.