Matemática Discreta

Quatrimestre de Primavera 2013

Lista 1 - Aritmética entera y modular

1. Convertir los siguiente números de base decimal a base binaria: 999_{10}, 1984_{10}. Convertir 10101111_2 i 101001000_2 de base binaria a decimal.

2. Expresar 706113_8 en base decimal y 89156_{10} en base octal.

3. La conversión del sistema binario al octal o al hexadecimal se puede hacer de una forma sencilla teniendo en cuenta que 8 i 16 son potencias de 2; encontrarla.

a) Convertir 2154_8 al sistema binario. Expresar 110100101_2 en base octal.

b) Convertir 100011110101_2 y 11101001110_2 al sistema hexadecimal. Expresar los números hexadecimals $ABCDEF_{16}$ y $9A0B_{16}$ en el sistema binario.

4. Sabemos que el número 136_{10} se expresa en la base b como 253. Encontrar la base b.

5. Buscar el MCD de las parejas de números siguientes usando el algoritmo de Euclides: (45, 75), (252, 198), (162, 222), (666, 1414), (721, 448) y (20785, 44350).

6. Expresar el MCD de 45 y 75 de la forma $45m + 75n$ con $m, n \in \mathbb{Z}$. Haced lo mismo con las demás parejas del problema anterior.

7. Calcular el MCM de 721 y 448 y de 20785 y 44350.
(Recordad: $\text{MCM}(a, b)\text{MCD}(a, b) = ab$.)

8. Dados dos números $a, b \in \mathbb{Z}$ coprimos, demostrar que el MCD de $a + b$ y $a^2 + b^2$ es 2 si a y b son impares y 1 en caso contrario.

9. Hemos instalado el sistema operativo Linux en dos particiones distintas: hda1 y hda2. Cada cierto número de veces que encendemos el ordenador se comprueban estas particiones. La partición hda1 se comprueba cada 31 veces y la partición hda2 cada 22 veces. Demostrar que alguna vez se comprueban ambas particiones simultáneamente. Calcular la frecuencia con la que se comprueban simultáneamente.

10. Buscar números enteros m, n tales que $966m + 686n = 70$.

11. El Dr. Fliess (conocido per su amistad y correspondencia con S. Freud) explica, en su libro *Der Ablauf des Lebens: Grundlegung zur exakten Biologie* que la vida humana está regida por un ciclo masculino de 23 dias y un ciclo femenino de 28. Este es el origen de la célebre teoría de los bioritmos. Concretamente, Fliess explica en su libro como muchos momentos críticos de la vida de una persona se pueden explicar sumando o restando un número entero de ciclos femeninos y masculinos. Demostrar que, en el momento en que el propio Fliess murió, el número de cabellos que tenía en la cabeza era suma o resta de un múltiplo de 23 y un múltiplo de 28, confirmando así su teoría.

12. Construir las tablas de sumar y de multiplicar de $\mathbb{Z}/8$.

13. Decir qué elementos son invertibles y cuáles son divisores de cero en $\mathbb{Z}/8$, $\mathbb{Z}/10$, $\mathbb{Z}/17$ y $\mathbb{Z}/24$.

14. Demostrar que un número es divisible por tres si y sólo si la suma de sus dígitos en base decimal es múltiplo de 3.

15. Sea n un número natural y sea $(x_k x_{k-1} \dots x_0)_{10}$ su representación en base 10. Sea $\theta(n) = x_0 + x_1 + \cdots + x_k$. Demostrar que

$$n \equiv \theta(n) \mod 9.$$

16. La conocida "prueba del 9" se basa en la propiedad $\theta(xy) \equiv xy \equiv \theta(x)\theta(y)$, consecuencia del problema anterior. Usar este hecho para demostrar que dos de los siguientes productos son erroneos. ¿Qué se puede decir del otro producto?

1. $5783 \times 40162 = 233256846$
2. $9787 \times 1258 = 12342046$
3. $8901 \times 5743 = 52018443$.

17. Calcular módulo 47 las potencias de 2 siguientes: 2^{32}, 2^{47}, 2^{200}.

18. Resolver las siguientes ecuaciones

$$\begin{array}{rcll} 2x & \equiv & 5 & (\text{mod } 7), \\ 3x & \equiv & 6 & (\text{mod } 9), \\ 19x & \equiv & 30 & (\text{mod } 40), \\ 9x & \equiv & 5 & (\text{mod } 25), \end{array} \qquad \begin{array}{rcll} 103x & \equiv & 444 & (\text{mod } 999), \\ 980x & \equiv & 1500 & (\text{mod } 1600), \\ 128x & \equiv & 833 & (\text{mod } 1001), \\ 987x & \equiv & 610 & (\text{mod } 1597). \end{array}$$

19. Encontrar una solución del sistema de ecuaciones

$$\begin{cases} x + 2y = 4 \\ 4x + 3y = 4 \end{cases}$$

en $\mathbb{Z}/7$. ¿Existe alguna solución en $\mathbb{Z}/5$?

20. Resolver la ecuación $x^2 - 3x - 3 = 0$ en $\mathbb{Z}/7$.

21. Buscar un número entero C no divisible por 11 y tal que la sucesión de números $a_n = C^n$ satisfaga la ecuación

$$a_n \equiv a_{n-1} + a_{n-2} \mod 11.$$

22. Buscar el último dígito de la expresión decimal de 7^{1000}.

23. Calcular $11^{289} \mod 360$ y $7^{418} \mod 120$

24. Resolver

$$\begin{array}{rcll} 5x & \equiv & 12 & (\text{mod } 13), \\ 7x & \equiv & 3 & (\text{mod } 11), \\ 5x & \equiv & 3 & (\text{mod } 14), \end{array} \qquad \begin{array}{rcll} 4x & \equiv & 7 & (\text{mod } 15), \\ 3x & \equiv & 5 & (\text{mod } 16), \end{array}$$

25. Calcular $\varphi(2000)$, $\varphi(2001)$, $\varphi(2002)$, $\varphi(2003)$ y $\varphi(2004)$.

26. Buscar una solución del sistema

$$\begin{cases} 10x \equiv 2 \mod 4 \\ 3x \equiv 1 \mod 5 \\ x \equiv 2 \mod 3 \end{cases}$$

27. Para hacer el recuento de las tropas después de una batalla, los generales chinos distribuían sus soldados en filas de diferente longitud y contaban la cantidad de soldados restantes en cada distribución. A partir de estos residuos calculaban el total. Un general tenía 1200 soldados al comenzar una batalla. Una vez terminada, le sobraban 3 soldados si formaban en filas de 5, sobraban 3 si las filas eran de 6, sólo sobraba uno si las filas eran de 7 y ninguno si las filas eran de 11. ¿Cuántos soldados sobrevivieron a la batalla?

28. Un pastor tiene un cierto número de ovejas. Nos ha dicho que si las cuenta de 2 en 2 sobra una, si las cuenta de 3 en 3 sobran 2, si las cuenta de 4 en 4 sobran 3, si las cuenta de 5 en 5 sobran 4, si las cuenta de 6 en 6 sobran 5 y si las cuenta de 7 en 7 sobran 6, pero no tiene más de 500 ovejas. ¿Cuántas ovejas tiene el pastor?

29. Codificar el mensaje

NO ENTREGUEIS ESTE SOBRE

usando el cifrado afín $C \equiv 7P + 10 \pmod{26}$

30. Decodificar el mensaje siguiente

KT VTULVTUDPT ADJPYLUT JDYQL CTYT PRADWDPTY VLGJTOLJ

que ha estado codificado usando el cifrado afín $C \equiv 11P + 19 \pmod{26}$.

31. Julio César solía usar congruencias para encriptar sus mensajes. Primero ordenaba alfabéticamente las 23 letras del alfabeto (latino romano) y asociaba a cada letra α su posición $p(\alpha)$, de 0 hasta 22. Así la letra A quedaba asociada al 0, la B al 1, la C al 2,.... Luego, sumaba 3 módulo 23 a las posiciones de las letras. Al final, cada letra α quedaba asociada al entero $p(\alpha) + 3 \pmod{23}$.
Vamos a usar como alfabeto el conjunto ordenado de sólo 7 letras (B,C,E,H,I,N,O). Para aplicar el método de César tendremos que trabajar módulo 7. ¿Cuál sería, en este caso, el sentido del mensaje 3051 65462?.

32. Se intercepta el texto cifrado:

FIUBVMUBZXBIUWCZH

que fue cifrado usando un código afín en el alfabeto de 27 letras (La A a Z de 0 a 25, y el espacio en blanco 26). Se sabe que la primera letra es L, y la segunda es O. Determinar la clave del cifrado y leer el mensaje.