Primer Parcial de Matemática Discreta 2, año 2001
SOLUCION DETALLADA

(**Para los ejercicios 1 y 2**) Se considera el anillo $(\mathbb{Z}_{40}, +, \cdot)$ de los enteros módulo 40. Se representan las letras desde " A " a " Z ", el espacio en blanco " $\square$ " el punto " · " , el signo de interrogación " ? " y los dígitos de " 0 "a " 9 " por los números:
A$\mapsto$ 0, B$\mapsto$ 1, C$\mapsto$ 2, D$\mapsto$ 3, E$\mapsto$ 4, F$\mapsto$ 5, G$\mapsto$ 6, H$\mapsto$ 7, I$\mapsto$ 8, J$\mapsto$ 9, K$\mapsto$ 10, L$\mapsto$ 11, M$\mapsto$ 12, N$\mapsto$ 13, Ñ$\mapsto$ 14, O$\mapsto$ 15, P$\mapsto$ 16, Q$\mapsto$ 17, R$\mapsto$ 18, S$\mapsto$ 19, T$\mapsto$ 20, U$\mapsto$ 21, V$\mapsto$ 22, W$\mapsto$ 23, X$\mapsto$ 24, Y$\mapsto$ 25, Z$\mapsto$ 26, $\square\mapsto$ 27, $\cdot \mapsto$ 28, ?$\mapsto$ 29, 0$\mapsto$ 30, 1$\mapsto$ 31, 2$\mapsto$ 32, 3$\mapsto$ 33, 4$\mapsto$ 34, $\quad 5 \mapsto 35,\ 6 \mapsto 36,\ 7 \mapsto 37,\ 8 \mapsto 38,\ 9 \mapsto 39$
Se cifra de a un carácter con un sistema afín $x \mapsto ax + b \ mod\ 40$.

1. (8 puntos) Hallar la clave (a, b) para que al cifrar la palabra "infiel" la "i" se transforme en "a" y la "f" se transforme en "8".

   Solución: La "i" se codifica con 8, la "a" con 0, la "f" con 5 y el "8" con 38 por lo que se tiene el sistema $\begin{cases} 8a + b & \equiv 0 \, mod\, 40 \\ 5a + b & \equiv 38 \, mod\, 40 \end{cases}$ Restando ambas ecuaciones queda: $3a \equiv -38 = 2 \, mod\, 40$ Por el AEE buscamos el inverso de 3 que es 27 o más fácil, $3 \times 13 = 39 = -1 \, mod\, 40$ y entonces directamente multiplicando por 13 queda $-a \equiv 2 \times 13 = 26 \, mod\, 40$. Luego $a \equiv -26 = 14 \, mod\, 40$. Con el valor de a hallamos b como $b \equiv -8a = 8 \times 26 = 8 \, mod\, 40$.

   Nota: el ejercicio originalmente pedía analizar si esta clave era buena para cifrar. La respuesta es NO, ya que 14 no es primo con 40. Se simplificó el ejercicio eliminando esa parte, no se exigió analizar la bondad o no de la clave.

   También puede resolverse aplicando el TChR escribiendo $40 = 8 \times 5$ y resolviendo las congruencias módulo 8 y módulo 5.

2. (8 puntos) Hallar la clave (a, b) para que al cifrar la palabra "ticholo" la "t" se transforme en "a" y la "h" se transforme en "s".

   Solución: $a \equiv -23 = 17 \, mod\, 40$. $b \equiv 20 \, mod\, 40$.

   Nota: el ejercicio originalmente pedía analizar si esta clave era buena para cifrar. La respuesta es SI, ya que 17 es primo con 40.

3. (8 puntos) Se considera la ecuación diofántica en $x, y \in \mathbb{Z}$ $ax+8y = 10$ Resolverla para $a = 2$, 3, 4 dando las soluciones para $-15 \leq x, y \leq 15$.

   Solución: Si $a = 2$ $MCD(2, 8) = 2$ y 2 divide a 10, luego hay solución. Es obvio que $(x_0, y_0) = (1, 1)$ es solución. En la ecuación diofántica $ax + by = c$, el

conocimiento de una solución permite escribir todas las soluciones como $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$, con $t \in \mathbb{Z}$ y $d = MCD(a, b)$. En este caso queda $x = 1 + 4t$, $y = 1 - t$. Además ambas variables x, y están entre -15 y 15. Luego debe ocurrir que a la vez $1 + 4t \leq 15$, $1 - t \leq 15$, $1 + 4t \geq -15$, $1 - t \geq -15$. La primera ecuación implica que $t \leq 7/2$, la segunda que $t \geq -14$ la tercera que $t \geq -4$ y la cuarta que $t \leq 16$. La intersección de todas las condiciones da, considerando que $t \in \mathbb{Z}$, que $-4 \leq t \leq 3$ o sea $t = -4, -3, -2, -1, 0, 1, 2, 3$. A partir de esto se pueden dar explícitamente los valores de (x, y). Obviamente, tomando otra solución particular van a quedar las mismas soluciones (x, y) pero pueden variar los valores de $t \in \mathbb{Z}$.

Si $a = 3$ $d = MCD(3, 8) = 1$ que divide a 10, luego hay solución. O bien aplicamos el AEE para escribir $d = 1$ como combinación entera de 3 y 8 y luego multiplicando por 10 tenemos una solución particular, o directamente buscamos adivinar una solución particular que en este caso es $(x_0, y_0) = (-2, 2)$. Toda otra solución se escribe como $x = -2+8t$, $y = 2-3t$, $t \in \mathbb{Z}$. Como x, y están entre -15 y 15 quedan las condiciones $-2 + 8t \leq 15$, $2 - 3t \leq 15$, $-2 + 8t \geq -15$, $2 - 3t \geq -15$. Esto da considerando que t es entero la intersección $t \leq 2$ y $t \geq -1$, o sea $t = -1, 0, 1, 2$. De aquí se obtienen las soluciones (x, y).

Si $a = 4$ queda $MCD(a, b) = MCD(4, 8) = 4$ que no divide a 10.Luego no existe solución.

4. (8 puntos) Se considera la ecuación diofántica en $x, y \in \mathbb{Z}$ $ax + 27y = 24$ Resolverla para $a = 3$, 5, 9 dando las soluciones para $-26 \leq x, y \leq 26$.

Solución: Valen consideraciones análogas que para el ejercicio anterior. Resulta que existen soluciones en los casos $a = 3$ y $a = 5$ pero no si $a = 9$.

Si $a = 3$ una solución particular es $(x_0, y_0) = (-1, 1)$. Toda otra solución se escribe como $x = -1 + 9t$, $y = 1 - t$, $t \in \mathbb{Z}$. Como tanto x como y están entre -26 y 26, queda $-2 \leq t \leq 3$.

Si $a = 5$ una solución particular es $(x_0, y_0) = (-6, 2)$. Toda otra solución es de la forma $x = -6 + 27t$, $y = 2 - 5t$, t solo puede valer 0 o 1.

Nota: Originalmente estos ejercicios tenían otra forma. Se pedía estudiar para qué valores de a las ecuaciones diofánticas $ax + 8y = 10$ y $ax + 27y = 24$ tenían solución.

5. (8 puntos) Hallar las soluciones, si existen, de

$$x^2 + 18x + 9 \equiv 0 \; mod \; 103$$

Solución: El módulo $p = 103$ es primo como surge de observar que no lo dividen ni 2

ni 3 ni 5 ni 7. Como $11^2 = 121 > 103$ con esto es suficiente. Completando cuadrados en la ecuación nos queda $x^2 + 18x + 9 = x^2 + 18x + 81 - 81 + 9 \equiv 0 \; mod \; 103$ o sea $(x+9)^2 \equiv 72 \; mod \; 103$. Una condición necesaria y suficiente para que exista solución de $y^2 \equiv \alpha \, mod \, p$ con $p > 2$ primo, es que $\alpha^{(p-1)/2} \equiv 1 \, mod \, p$. Calculamos entonces $72^{51} \, mod \, 103$.Para ello utilizamos el algoritmo de exponenciación veloz. Escribimos entonces 51 en base 2 como $51 = 32 + 16 + 2 + 1 = 2^5 + 2^4 + 2^1 + 2^0 = (110011)_2$. Calculamos ahora por elevación al cuadrado repetidas veces cuánto vale $72^2 \, mod \, 103$, $72^4 \, mod \, 103, \ldots, 72^{32} \, mod \, 103$.

$$72^2 = 5184 = 34 \, mod \, 103, \quad 72^4 = 34^2 = 1156 = 23 \, mod \, 103$$

$$72^8 = 23^2 = 529 = 14 \, mod \, 103 \quad 72^{16} = 14^2 = 196 = 93 \, mod \, 103$$

$$72^{32} = 93^2 = 8649 = 100 \, mod \, 103$$

Resulta

$$72^{51} = 72^{32}72^{16}72^272 = 100 \times 93 \times 34 \times 72 \equiv 1 \, mod \, 103$$

Existe entonces un valor de x tal que $(x+9)^2 \equiv 72 \, mod \, 103$. Para hallarlo observamos que $103 = 100 + 3 \equiv 3 \, mod \, 4$ y recordamos que si $y^2 \equiv \alpha \, mod \, p$ tiene solución y $p \equiv 3 \, mod \, 4$ entonces una de las soluciones b se calcula como $b = \alpha^{(p+1)/4} \, mod \, p$ siendo $-b \, mod \, p$ la otra solución. En este caso $(p+1)/4 = 26 = 16 + 8 + 2$ y aplicamos el algoritmo de exponenciación otra vez. Considerando que los valores de $72^{2^h} \, mod \, 103$ ya los calculamos antes queda

$$b = 72^{16}72^872^2 = 93 \times 14 \times 34 \equiv 81 \, mod \, 103$$

Por lo que $x + 9 = 81 \, mod \, 103$ y $x = 72 \, mod \, 103$ es solución. La otra es $x + 9 = -81 = 103 - 81 = 22$ que da $x = 22 - 9 = 13 \, mod \, 103$. Se puede comprobar que efectivamente son solución sustituyendo en $x^2 + 18x + 9$ los valores $x = 72$ y $x = 13$ y viendo que el resultado es 0 módulo 103.

6. (8 puntos) Hallar las soluciones, si existen, de

$$x^2 + 18x + 20 \equiv 0 \; mod \; 107$$

Solución: Es enteramente análogo al ejercicio anterior. También aquí 107 es primo y es congruente con 3 módulo 4. Al completar cuadrados se obtiene $(x + 9)^2 \equiv 61 \, mod \, 107$ Para averiguar si hay solución calculamos $61^{53} \, mod \, 107$. $53 = 32 + 16 + 4 + 1 = 2^5 + 2^4 + 2^2 + 1$. Obtenemos

$$61^2 \equiv 83 \, mod \, 107 \quad 61^4 \equiv 41 \, mod \, 107 \quad 61^8 \equiv 76 \, mod \, 107$$

$$61^{16} \equiv 105 \equiv -2 \, mod \, 107 \quad 61^{32} \equiv 4 \, mod \, 107$$

Otra vez queda $61^{53} \equiv 1 \, mod \, 107$. Para hallar una solución calculamos $61^{27} \, mod \, 107$ obteniendo $x + 9 = 75 \, mod \, 107$. Queda $x \equiv 66 \, mod \, 107$ y la otra solución se obtiene despejando x en $x + 9 = -75 \, mod \, 107$. Queda $x = -84 = 107 - 84 = 23 \, mod \, 107$.

7. (8 puntos) Un cocinero es nuevo en un restorán. Al llegar el proveedor de huevos olvida preguntar cuantos dejó. El cocinero se da cuenta que habiéndolos dividido en docenas sobran 2 huevos. Los ayudantes le dicen que cuando traen el doble y hacen tortillas (que llevan 7 huevos c/u) sobran 3 y cuando traen el triple, que es cuando hacen tortas (que llevan 5 huevos c/u), sobra 1 huevo. Finalmente se fija que las cajas dicen "capacidad máxima 400 huevos". ¿Cuántos huevos son si lo que dejó el proveedor entraba en una caja?

Solución: Es una aplicación estándar del TChR. Queda el sistema: $\begin{cases} x & \equiv 2 & mod \, 12 \\ 2x & \equiv 3 & mod \, 7 \\ 3x & \equiv 1 & mod \, 5 \end{cases}$

El inverso de 2 módulo 7 es 4 por lo que escribimos la segunda ecuación como $x \equiv 4 \times 3 = 5 \, mod \, 7$ y el inverso de 3 módulo 5 es 2 por lo que la tercera ecuación queda $x \equiv 2 \times 1 = 2 \, mod \, 5$. Al final queda $\begin{cases} x & \equiv 2 & mod \, 12 \\ x & \equiv 5 & mod \, 7 \\ x & \equiv 2 & mod \, 5 \end{cases}$ Definimos $M = 12 \times 7 \times 5 = 420$, $M_1 = 7 \times 5 = 35$, $M_2 = 12 \times 5 = 60$, $M_3 = 12 \times 7 = 84$. $N_1 = 35^{-1} \, mod \, 12 = 11$, $N_2 = 60^{-1} \, mod \, 7 = 2$ $N_3 = 84^{-1} \, mod \, 5 = 4$ Una solución módulo $M = 420$ se obtiene como $x = 2 \times 35 \times 11 + 5 \times 60 \times 2 + 2 \times 84 \times 4$ que da $x = 2042 \, mod \, 420 = 362$.

8. (8 puntos) Un cocinero es nuevo en un restorán. Al llegar el proveedor de huevos olvida preguntar cuantos dejó. El cocinero se da cuenta que habiéndolos dividido en docenas sobran 3 huevos. Los ayudantes le dicen que cuando traen el doble y hacen tortillas (que llevan 7 huevos c/u) sobra 1 huevo y cuando traen el triple, que es cuando hacen tortas (que llevan 5 huevos c/u) no sobra nada. Finalmente se fija que las cajas dicen "capacidad máxima 400 huevos". ¿Cuántos huevos son si lo que dejó el proveedor entraba en una caja?

Solución: Queda $x = 375 \, mod \, 420$.

9. (8 puntos) Un elemento $a \in \mathbb{Z}_N$, $a \neq 0$, se dice nilpotente si existe $m > 1$, natural, tal que $a^m \equiv 0 \; mod \; N$. Sea $N = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}$ la descomposición factorial de N, $1 \leq h_j$.

(a) Probar que si existe j tal que el exponente h_j de p_j es mayor que 1, entonces existe $a \in \mathbb{Z}_N$ que es nilpotente.

Prueba: Tomemos $a = p_1 p_2 \cdots p_k$. Como existe un $h_j > 1$ se cumple $0 < a < N$ y $a \neq 0 \, mod \, N$. Elevando a a la potencia $m = \max\{h_1, h_2, \ldots h_k\}$ se tiene que $a^m \equiv 0 \, mod \, N$. En efecto, $a^m = (p_1 p_2 \cdots p_k)^m = p_1^m p_2^m \cdots p_k^m$. Como $h_i \leq m$ resulta $a^m = \dot{N}$ y $a^m \equiv 0 \, mod \, N$

(b) Probar que si $h_j = 1$ para todo $j = 1, \ldots, k$ entonces no existen elementos nilpotentes en $\mathbb{Z}_N$.

Prueba: Si $a \in \mathbb{Z}_N$ cumple que $a^m \equiv 0 \, mod \, N$ entonces $a^m = \dot{N}$. De aquí que cualquier primo p_i divide a $a^m = a^{m-1}a$. Como p_i es primo debe dividir a algún factor, o bien a a o bien a a^{m-1}. Si divide a a^{m-1} y $m - 1 > 1$ escribimos $a^{m-1} = a^{m-2}a$ y repetimos la argumentación, debe dividir a a o a a^{m-2}. Si divide a a^{m-2} volvemos a escribir $a^{m-2} = a^{m-3}a$ y argumentamos de nuevo de la misma forma. Como $m > m - 1 > m - 2 > \ldots$ es una sucesión decreciente positiva, finalmente encontramos que p_i debe dividir siempre a a. Hemos probado que para todo i p_i divide a a. Entonces, como los p_i son primos distintos entre sí dos a dos resulta que el producto $p_1 p_2 \cdots p_k = N$ también debe dividir a a. O sea que $a = \cdot N$ y eso es lo mismo que decir que $a \equiv 0 \, mod \, N$. Luego no hay $a \neq 0$ en $\mathbb{Z}_N$ tales que $a^m = 0$ con algún $m > 1$.