Solucíon del 1er parcial de MATEMÁTICA DISCRETA 2. Mayo 2012

Ejercicio 1.

A. Como $\text{mcd}(a,b) = 1$, por Bezout tenemos que existen $x, y \in \mathbb{Z}$ tal que $1 = ax + by$. Multiplicando por c tenemos que $c = acx + bcy$. Ahora, como $a|c$ tenemos que $ab|bc$ y por lo tanto $ab|bcy$. Por otro lado, como $b|c$, entonces $ab|ac$ y entonces $ab|acx$. Así que ab divide a bcy y a acx y por lo tanto divide a $acx + bcy = c$.

También se puede probar a partir del Lema de Euclides o usando las descomposiciones en factores primos de a y b.

B. Ver teórico

C. Sabemos que una solución al sistema es $x_0 = 1(8)9a + 0(5)9b + 1(5)8c$ con

$(8)9a \equiv 1 \mod (5) \Rightarrow 72a \equiv 1 \mod (5) \Rightarrow 2a \equiv 1 \mod (5) \Rightarrow a \equiv 3 \mod (5)$

$(5)8c \equiv 1 \mod (9) \Rightarrow 40c \equiv 1 \mod (9) \Rightarrow 4c \equiv 1 \mod (9) \Rightarrow c \equiv -2 \mod (9)$

Así que una solución es $x_0 = 1(8)9(3) + 1(5)8(-2) = 216 - 80 = 136$ y toda solución es $x = 136 + k(5)(8)(9) = 136 + 360\,k$ con $k \in \mathbb{Z}$. Así que el menor natural que verificala ecuación es $x = 136$.

D. Como 8 y 5 son coprimos tenemos que $x \equiv 16 \pmod{40} \Leftrightarrow \begin{cases} x \equiv 16 \pmod 8 \\ x \equiv 16 \pmod 5 \end{cases} \Leftrightarrow$ $\begin{cases} x \equiv 0 \pmod 8 \\ x \equiv 1 \pmod 5 \end{cases}$. Como 5 y 3 son coprimos tenemos que $x \equiv 1 \pmod{15} \Leftrightarrow \begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \end{cases}$, y como 9 y 2 son coprimos tenemos que $x \equiv 10 \pmod{18} \Leftrightarrow \begin{cases} x \equiv 10 \pmod 9 \\ x \equiv 10 \pmod 2 \end{cases} \Leftrightarrow$ $\begin{cases} x \equiv 1 \pmod 9 \\ x \equiv 0 \pmod 2 \end{cases}$. Así que el primer sistema es equivalente al sistema: $\begin{cases} x \equiv 0 \pmod 8 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 9 \\ x \equiv 0 \pmod 2 \end{cases}$

Ahora, si $x \equiv 1 \pmod 9 \Rightarrow x \equiv 1 \pmod 3$ y si $x \equiv 0 \pmod 8 \Rightarrow x \equiv 0 \pmod 2$; por lo tanto, si x verifica la penúltima ecuación, verifica la tercera (entonces no necesitamos la tercer ecuación) y si x verifica la primer ecuación, entonces verifica la última (y no necesitamos la última ecuacion en el sistema; además, la ecuación con congruencia módulo 5 apareció repetida. Así que el sistema es equivalente al sistema:

$\begin{cases} x \equiv 0 \pmod 8 \\ x \equiv 1 \; (\text{mod}\, 5 \\ x \equiv 1 \pmod 9 \end{cases}$. Este es el sistema de la parte A. así que las soluciones son $x = 136 + 360k$, $k \in \mathbb{Z}$.

Para el segundo sistema: Si $x \equiv 6 \pmod{15} \Rightarrow x \equiv 6 \pmod 3 \Rightarrow x \equiv 0 \pmod 3$ Como vimos para el primer sistema, la ecuación $x \equiv 10 \pmod{18}$ implica que $x \equiv 1 \pmod 3$. Por unicidad del resto al dividir entre 3, no existe un x que verifique estas ecuaciones y por lo tanto el sistema no tiene solución.

Ejercicio 2.

A. Como $2^n + 7^n$ es impar (si fuera par se tendría que $2|7$), si $d|2^n + 7^n$, entonces d es impar. Si además $d|(2^n - 7^n) \Rightarrow d|(2^n + 7^n + 2^n - 7^n) = 2^{n+1}$. Luego $d = 2^h$ para $0 \leq h \leq n+1$. La única tal potencia de 2 que es impar es 1. Así que $\text{mcd}(2^n + 7^n, 2^n - 7^n) = 1$.

B. Si la descomposición en factores primos de n es $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$, entonces la cantidad de divisores positivos de n es $\prod_{i=1}^{k}(a_i + 1)$. Así que $\prod_{i=1}^{k}(a_k + 1) = 30 = 2 \cdot 3 \cdot 5$. Así que (por ser 2,3, y 5 primos) algún $a_i + 1 = 2$, otro es 3, otro es 5 y el resto son 1. Por lo que algún $a_1 = 1$, otro es 2,otro es 4 y el resto son 0. Por lo tanto $n = p_1 \cdot p_2^2 \cdot p_3^4$ con los p_i primos distintos.

Por otro lado, como $\operatorname{mcd}(n, 1260) = 70$ tenemos que $n = 70k$ con $\operatorname{mcd}(k, 1260/70) = 1$, es decir $\operatorname{mcd}(k, 18) = 1$. Así que $n = 2 \cdot 5 \cdot 7k$ con k coprimo con 2 y con 3.

Juntando ambas conclusiones tenemos que $n = 2 \cdot 5^a \cdot 7^b$ con $(a, b) = (2, 4)$ o $(a, b) = (4, 2)$.

C. Veamos dos formas de resolverlo: Como $\varphi(3^n) = 2 \cdot 3^{n-1}$, entonces por el Teo. de Eüler tenemos que si $\operatorname{mcd}(a, 3^{n-1}) = 1$ entonces $a^{2 \cdot 3^{n-1}} \equiv 1 \mod (3^n)$. Tomando $a = 8$ tenemos que $8^{2 \cdot 3^{n-1}} \equiv 1 \mod (3^n)$; así que $\left(8^2\right)^{3^{n-1}} \equiv 1 \mod (3^n)$ y por lo tanto $64^{3^{n-1}} \equiv 1 \mod (3^n)$, es decir 3^n divide a $64^{3^{n-1}} - 1$.

Otra forma de resolver el ejericio es por inducción en n el caso $n = 1$ es cierto porque 3 divide a $64 - 1 = 63$.

Para simplificar, llamémosle $a = 64^{3^{n-1}}$. Si 3^n divide a $64^{3^{n-1}} - 1$, (es decir que 3^n divide a $a-1$), queremos probar que 3^{n+1} divide a $64^{3n} - 1 = a^3 - 1$. Como 3^n divide a $a-1$, tenemos que $a = 1 + h \cdot 3^n$ para algún $h \in \mathbb{Z}$. Usando que $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$, tenemos que $a^3 = (1 + h \cdot 3^n)^3 = 1 + 3h \cdot 3^n + 3h^2 \cdot 3^{2n} + h^3 \cdot 3^{3n} = 1 + h \cdot 3^{n+1} + h^2 3^n 3^{n+1} + h^3 3^{2n-1} 3^{n+1}$. Así que $3^{n+1} \mid a^3 - 1$, probando la tesis de inducción.

Ejercicio 3.

A. Ver teórico.

B. Tenemos que hallar todos los $c \in \mathbb{Z}$ tales que $9c \equiv 1 \mod (1190)$; es decir, los $c \in \mathbb{Z}$ para los cuales existe $k \in \mathbb{Z}$ tal que $9c + 1190k = 1$. Resolvemos esta ecuación diofántica: hallamos una solución particular utilizando el Algoritmo de Euclides Extendido: Como $1190 = 9(132) + 2$ y $9 = 4(2) + 1$ obtenemos que $1 = 9 - 4(2) = 9 - 4(1190 - 9(132)) = 9(1 + 4(132)) + 1190(-4) = 9(529) + 1190(-4)$. Por lo tanto una solucón particular es $(c_0, k_0) = (529, -4)$ y y por la parte A, como $\operatorname{mcd}(9, 1190) = 1$ tenemos que todas las soluciones son $(c, k) = (529 + 1190h, -4 - 9h)$ $h \in \mathbb{Z}$. Asi que los inversos de 9 módulo 1190 son $c = 529 + 1190h$, $h \in \mathbb{Z}$

C. Buscamos $x \in \{0, 1 \cdots, 1189\}$ tal que $x \equiv 3^{382} \mod (1190)$. Como $1190 = 2 \cdot 5 \cdot 7 \cdot 17$ enconces $\varphi(1190) = 1 \cdot 4 \cdot 6 \cdot 16 = 384$. Como $\operatorname{mcd}(3, 1190) = 1$, por el teorema de Eüler tenemos que $3^{384} \equiv 1 \mod (1190)$. Así que si $x \equiv 3^{382} \mod (1190) \Rightarrow 9x = 3^2 x \equiv 3^2 3^{382} \mod (1190) \Rightarrow 9x \equiv 3^{384} \mod (1190)$ y por lo tanto $9x \equiv 1 \mod (1190)$. Así que buscamos $x \in \{0, 1 \cdots, 1189\}$ tal que x es inverso de 9 módulo 1190. Por la parte anterior, tenemos que $x = 529$.