Soluciones del examen de Conjuntos y Números del 18 de enero de 2012

1) a) Escribiendo $6k-1 = 6(k-1)+5$, el enunciado es equivalente a probar que cualquier entero positivo $6n+5$ tiene un factor primo de la forma $6m+5$.

Sea p un factor primo de $6n+5$ y sea a su resto al dividir por 6, es decir $p \equiv a \pmod 6$. No puede ser $a = 0$ (porque no hay primos divisibles por 6) ni $a = 2, 4$ porque el único primo par, $p = 2$, no divide a $6n+5$. De la misma forma, $a = 3$ también es imposible porque $p = 3$ es el único primo múltiplo de 3 y no divide a $6n+5$. Las únicas posibilidades son entonces $p \equiv 1 \pmod 6$ y $p \equiv 5 \pmod 6$.

Si todos los factores primos de $6n+5$ cumplieran $p \equiv 1 \pmod 6$, entonces el propio $6n+5$, que es producto de ellos, también lo cumpliría, lo cual es absurdo porque $6n+5 \equiv 5 \pmod 6$.

b) Los números $2, 3, 4, \ldots, n$ dividen a $6n!$ y por tanto no pueden dividir a $6n!-1$. Entonces todo factor primo es mayor que n y por a) sabemos que alguno de ellos es de la forma $6m-1$.

2) Recordemos que una función se dice que es biyectiva cuando es inyectiva y sobreyectiva, y esto equivale a que tenga inversa.

a) Comprobamos las tres propiedades.

Reflexiva: $A\mathcal{R}A$ se cumple porque la función identidad $\mathrm{Id} : A \longrightarrow A$, $\mathrm{Id}(x) = x$ es una biyección (obvio).

Simétrica: $A\mathcal{R}B \;\Rightarrow\; A\mathcal{R}B$ porque si $f : A \longrightarrow B$ es biyectiva, entonces $f^{-1} : B \longrightarrow A$ también lo es (f^{-1} es sobre porque $x = f^{-1}\big(f(x)\big)$ y es inyectiva porque $f^{-1}(x) = f^{-1}(y) \Rightarrow x = y$, aplicando f).

Transitiva: $A\mathcal{R}B \;\wedge\; B\mathcal{R}C \;\Rightarrow\; A\mathcal{R}C$ porque si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son biyectivas, entonces $g \circ f : A \longrightarrow C$ también lo es (ya que tiene inversa $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$).

b) Por definición, estarán relacionados los subconjuntos no vacíos de $\mathbb{N}$ que tienen el mismo cardinal. Si un subconjunto de $\mathbb{N}$ es infinito necesariamente es biyectivo a $\mathbb{N}$ (esto se sigue ordenando sus elementos y asignado al primero el 0, al segundo el 1 y así sucesivamente). Por otro lado, si un conjunto es finito, digamos de cardinal n, es biyectivo a $C_n = \{1, 2, \ldots, n\}$. En definitiva, el conjunto cociente es $\mathcal{C} = \{\overline{\mathbb{N}}, \overline{C_1}, \overline{C_2}, \overline{C_3}, \ldots\}$ donde $\overline{A}$ indica la clase de A. El cardinal de $\mathcal{C}$ es $\aleph_0$ ya que podemos establecer la biyección $F : \mathbb{N} \longrightarrow \mathcal{C}$ mediante $F(0) = \overline{\mathbb{N}}$ y $F(n) = \overline{C_n}$ para $n \geq 1$.

3) a) Supongamos $\sqrt{3} = a/b$ con a/b una fracción irreducible. Entonces $3b^2 = a^2$ implica $3 \mid a$ y por tanto $9 \mid a^2$, pero como a y b son coprimos, $9 \nmid 3b^2$ y se llega a una contradicción.

b) La congruencia $37x \equiv 2012 \pmod{10000}$ tiene solución $x \in \mathbb{N}$ porque $\mathrm{mcd}(2012, 37) = 1$ (de hecho tiene exactamente una con $0 \leq x < 10000$), entonces $N = 37x$ es el número buscado ya que es múltiplo de 37 y de la forma $N = 10000k + 2012$.

4) a) Aplicando el algoritmo de Euclides:

$$\begin{cases} p(X) = q(X)(X+1) + (X^2+X+1) \\ q(X) = (X^2+X+1)(X+2) + 0 \end{cases}$$

Entonces $\mathrm{mcd}\big(p(X), q(X)\big) = X^2 + X + 1$.

b) Según el segundo paso del algoritmo de Euclides, $q(X) = (X^2+X+1)(X+2)$. La ecuación $X^2 + X + 1 = 0$ tiene raíces complejas $(-1 \pm i\sqrt{3})/2$, entonces $q(X) = (X^2 + X + 1)(X + 2)$ es la descomposición en irreducibles en $\mathbb{R}[X]$, mientras que en $\mathbb{C}[X]$ se tiene la descomposición $q(X) = \big(X - (-1 + i\sqrt{3})/2\big)\big(X - (-1 - i\sqrt{3})/2\big)(X + 2)$.

5) Recordemos que una función inyectiva F es la que cumple $F(x) = F(y) \;\Rightarrow\; x = y$.

a) Si $h(x) = h(y)$ entonces $f(x) = f(y) \;\wedge\; g(x) = g(y)$. Si f ó g son inyectivas esto implica $x = y$ y se deduce que h es inyectiva.

b) Por ejemplo, tomemos $X = \{0, 1, 2, 3\}$, $Y = Z = \{0, 1\}$ y f y g dando el *bit* más y menos significativo, es decir $g(0) = g(2) = f(0) = f(1) = 0$ y $g(1) = g(3) = f(2) = f(3) = 1$. Entonces $h(0) = (0, 0)$, $h(1) = (0, 1)$, $h(2) = (1, 0)$, $h(3) = (1, 1)$, que claramente es biyectiva (inyectiva y sobreyectiva).