**Universidad de la República**
**Facultad de Ingeniería**
**Instituto de Matemática y Estadística**

**Matemática Discreta 2**
**Curso 2009**

Primer parcial de Matemática Discreta 2.
2 de Mayo de 2009

| Número de Examen | Cédula | Nombre y Apellido |
|---|---|---|
| | | |

**Ejercicio 1.**

a) Hallar todos los $x$ e $y \in \mathbb{Z}$ tales que $26x + 11y = 1$.

Usando el AEE llegamos a la ecuación $3 \cdot 26 - 7 \cdot 11 = 1$ (obs. de aqui se concluye que $3 \cdot 26 \equiv 1 \pmod{11}$ y que $11 \cdot (-7) \equiv 1 \pmod{11}$). Por teorema visto en clase todas las soluciones vienen dadas por:

$$\begin{cases} x = 3 - 11t \\ y = -7 + 26t \end{cases}$$

con $t \in \mathbb{Z}$.

b) Se tiene las siguientes afirmaciones para $x \in \mathbb{Z}$:

i) $x \equiv 133^{196} \pmod{26}$

ii) El dígito menos significativo en base 11 es 6.

Se pide hallar todos los valores de $x$ que verifican las condiciones i) y ii).
¿Hay alguno de los valores que sea múltiplo de 22?

Primero observamos que $133^{196} \equiv 3^{196} = (3^{12})^{16} \cdot 3^4 \equiv 3^4 \equiv 3 \pmod{26}$ (se usó que $3^{12} \equiv 1 \pmod{26}$ que es consecuencia de Fermat-Euler). El sistema a resolver nos queda:

$$\begin{cases} x \equiv 3 \pmod{26} \\ y \equiv 6 \pmod{11} \end{cases}$$

asi que por el Teorema del resto chino, una solución viene dada por $A = 3 \cdot 11 \cdot (-7) + 6 \cdot 26 \cdot 3 = -231 + 468 = 237$ por lo tanto $x \equiv 237 \pmod{286}$.
Observar que $x \equiv 6 \pmod{11}$ implica que $x$ no puede ser múltiplo de 11, por lo tanto ningún $x$ que verifique i) y ii) puede ser múltiplo de 22.

**Ejercicio 2.**

a) Sea $(G, \cdot)$ un grupo.

i) Definir el orden de un elemento de $G$.

ii) Probar que el orden de $g \in G$ es igual al orden del subgrupo generado por $g$ (es decir que $o(g) = |\langle g \rangle|$).

Demostración vista en Teórico.

b) Sea $H = \{f : \mathbb{R} \to \mathbb{R} : f \text{ biyectiva}\}$.

i) Probar que $(H, \circ)$ es un grupo (la operación $\circ$ es la composición). Observar que composición de funciones biyectivas continua siendo una función biyectiva, que la función identidad definida por $e(x) = x$ para todo $x \in \mathbb{R}$ es el elemento neutro y que como las funciones de $H$ son biyectivas, son también invertibles (por lo tanto todo elemento de $H$ tiene inverso). Para chequear la asociativa tomemos $x \in \mathbb{R}$, tenemos que $(f \circ g) \circ h(x) = f \circ g(h(x)) = f(g(h(x)))$ y que $f \circ (g \circ h)(x) = f(g \circ h(x)) = f(g(h(x)))$. Como vale para todo $x \in \mathbb{R}$ se tiene que $(f \circ g) \circ h = f \circ (g \circ h)$.

ii) Sean $h, g : \mathbb{R} \to \mathbb{R}$ definidas por $h(x) = x^3 + 1$ y $g(x) = -x$.
Hallar $o(g)$ y $o(h)$ (donde $o(f)$ denota el orden de $f$ en el grupo $H$).
Probaremos por inducción que $gr(h^n) = 3^n$ para todo $n \in \mathbb{Z}^+$, donde $h^n = h \circ h \circ h \circ \ldots \circ h$ es la composición de $h$ consigo misma $n$ veces.
Para $n = 1$ es cierto ($gr(h) = 3$), si se verifica para $n$ entonces $h^{n+1}(x) = h(h^n(x)) = h^{n3} + 1$ luego $gr(h^{n+1}) = 3gr(h^n) = 3 \cdot 3^n = 3^{n+1}$. Como $gr(e) = 1$ se deduce que no existe ningún $n \in \mathbb{Z}^+$ tal que $h^n = e$ y por lo tanto $h$ tiene orden infinito. Por otra parte $g(g(x)) = g(-x) = x$ por lo tanto $g^2 = e$ y su orden es 2.

**Ejercicio 3.**

a) Definir pseudoprimo (o número) de Carmichael.

b) (Teorema de Korselt) Demostrar que si para todo factor primo $p|n$ se tiene que $p^2$ no divide a $n$ y $p - 1$ divide a $n - 1$ entonces $n$ es un número de Carmichael.

Visto en teórico.

c) Decidir si cada una de las siguientes afirmaciones son verdaderas o falsas (justificar):

i) $5^{560} \equiv 1 \pmod{561}$.

ii) $11^{560} \equiv 1 \pmod{561}$

Como $561 = 3 \cdot 11 \cdot 17$ y $2, 10$ y $16$ son divisores de 560 resulta que 561 es de Carmichael, por lo tanto $5^{561} \equiv 5 \pmod{561}$ dividiendo entre 5 de ambos lados (obs que 5 y 561 son coprimos) tenemos que $5^{560} \equiv 1 \pmod{561}$ por lo tanto la primera es verdadera.
Por otra parte si $11^{560} \equiv 1 \pmod{561}$ entonces $11^{560} \equiv 1 \pmod{11}$ por lo que $11^{560}$ no sería múltiplo de 11 lo cual es falso.