

Examen de Matemática Discreta II

27 de febrero de 2008

Número de Examen	Cédula	Nombre y Apellido

1. (30 puntos)

- a) En el cambio de turno de una fábrica de cerámicas, Alex, obrero que finalizaba su trabajo, dejó preparado un embarque de baldosas para un hospital en construcción. Armó una caja de 42 baldosas y dejó escrito: “Negro: va esta caja de 42 unidades y el resto son cajas de 50 unidades”. El Negro García, luego de subir al camión la de 42, comenzó a colocar las de 50 unidades, cuando se preguntó: ¿cuántas de 50 hay que llevar? Subió a Administración, donde el Pelado Fernández le ayudó a buscar la información y le avisó que el sabía que eran entre 20 y 40 cajas. Lo único que encontraron era un papel que decía: “Baldosas de cerámica para el Hospital psiquiátrico **Cristóbal Colón**. Salas de 32 baldosas + una sala chica de 20 baldosas”.
- ¿Cuántas baldosas precisa el hospital?
- b) Sea  $n$  el número de baldosas solución de la parte anterior. Hallar  $n \neq m \in \mathbb{N}$  tal que  $\phi(m) = \phi(n)$ , siendo  $\phi$  la función de Euler.

2. (35 puntos)

Consideramos el grupo  $G = (\mathbb{Z}_p^*, \cdot)$  con  $p > 2$  primo. Un elemento  $x \in \mathbb{Z}_p^*$  es un resto cuadrático si  $x = y^2$  para algún  $y \in \mathbb{Z}_p^*$ .

- a) Calcular los restos cuadráticos en  $\mathbb{Z}_7^*$ .
- b) Probar que  $\phi : G \rightarrow G$  definida por  $\phi(x) = x^2$  es un morfismo de grupos y calcular su núcleo.
- c) Probar que  $H = \{ x \in \mathbb{Z}_p^* \mid x \text{ es resto cuadrático} \}$  es subgrupo de  $\mathbb{Z}_p^*$  y que  $\frac{\mathbb{Z}_p^*}{\{\pm 1\}} \cong H$ . Contar cuántos de los elementos de  $\mathbb{Z}_p^*$  son restos cuadráticos.
- d) Observar que  $H \triangleleft \mathbb{Z}_p^*$  y determinar  $\mathbb{Z}_p^*/H$ . Construir la tabla de multiplicación.
- e) Probar que el producto de dos elementos que no son restos cuadráticos es siempre un resto cuadrático.

3. (35 puntos)

(Este ejercicio pretende mostrar una falla de protocolo cuando se utiliza el criptosistema RSA).

- a) Enunciar el criptosistema RSA.
- b) Supongamos que  $n$  es un número muy difícil de factorizar. Bernardo utiliza un criptosistema RSA con clave  $(n, e_1)$ , al mismo tiempo que Bruno utiliza la clave  $(n, e_2)$ , con  $\text{mcd}(e_1, e_2) = 1$ . Adriana les envía el mismo texto  $x$  a ambos, calculando  $y_1 = x^{e_1} \text{mod}(n)$  e  $y_2 = x^{e_2} \text{mod}(n)$  (envía  $y_1$  a Bernardo e  $y_2$  a Bruno). Alguien que intercepta los mensajes realiza los siguientes cálculos:
- $c_1 = e_1^{-1} \text{mod}(e_2)$ ;
  - $c_2 = \frac{c_1 \cdot e_1 - 1}{e_2}$ ;
  - $x_1 = y_1^{c_1} (y_2^{c_2})^{-1} \text{mod}(n)$ .
- i) Probar que  $x_1$  calculado en el paso 3 es el texto  $x$ . Por lo tanto, si bien el criptosistema es seguro, el mensaje puede ser descifrado en este caso.
- ii) Descifrar el mensaje si  $y_1 = 9983$  e  $y_2 = 4026$ , sabiendo que  $n = 16123$ ,  $e_1 = 27$  y  $e_2 = 29$ . (Se sugiere utilizar el algoritmo de exponenciación rápida).