

Examen de Matemática Discreta II
3 de Mayo de 2008

Número de Examen	Cédula	Nombre y Apellido

Ejercicio 1.

Sea φ la indicatriz de Euler y consideremos el conjunto $A = \{m \in \mathbb{Z}^+ : \varphi(m) | m - 1\}$.

- Probar que el conjunto A posee infinitos elementos.
- Probar que si $m \in A$ entonces $m = 1$ o bien m es producto de primos distintos (o sea que no existe un primo p tal que $p^2 | m$).
- Probar que si $m = pq$ donde p y q son primos distintos entonces $m \notin A$.

Ejercicio 2.

Supongamos que utilizamos el criptosistema RSA con claves públicas (n, e) con $31^2 < n < 31^3$, utilizando un protocolo de encriptación por bloques que se describe a continuación.

Para encriptar separamos el texto en bloques de 2 caracteres, por ejemplo, si el texto es "DISCRETA" nos quedan 4 bloques "DI", "SC", "RE", "TA". Luego a cada bloque le hacemos corresponder un entero entre 0 y $31^2 - 1$ como vimos en clase (la tabla que asigna a cada caracter un número está dada más adelante). Para encriptar el texto lo hacemos bloque a bloque, si x es el número correspondiente a un bloque, $E(x)$ está entre 0 y $n - 1 < 31^3$, luego podemos verlo como un número de 3 cifras en base 31 (agregando ceros al principio de ser necesario), luego corresponde a un bloque de 3 caracteres (el bloque encriptado).

Para desencriptar dividimos el texto en bloques de a 3 caracteres, representando a cada bloque con un número del 0 al $31^3 - 1$ y desencriptamos bloque a bloque, si y es el número correspondiente a un bloque encriptado, $D(y)$ estará entre 0 y $31^2 - 1$, luego representará un bloque con 2 caracteres (el bloque desencriptado).

La tabla que asigna a cada caracter un elemento de \mathbb{Z}_{31} es la siguiente:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
V	W	X	Y	Z			?	!	¿												
22	23	24	25	26	27	28	29	30													

Se ha interceptado el siguiente mensaje THGS!H enviado por Alicia. Al buscar la clave de Alicia, ésta es (27221, 24623). Alicia ha escogido mal los parámetros y se ha podido factorizar n de la siguiente forma $n = 167 \cdot 163$.

- ¿Por qué se puede afirmar que los parámetros fueron mal escogidos?
- Desencripte el mensaje enviado por Alicia (sugerencia: Teorema del resto chino y teorema de Fermat).

Ejercicio 3.

- a) Sean a y m enteros positivos coprimos y $S = \{n \in \mathbb{Z}^+ : a^n \equiv 1 \pmod{m}\}$
- Probar que $S \neq \emptyset$.
 - Probar que si $s = \min S$ y $n \in S$ entonces $s|n$.
- b) Sean p y q primos distintos, a un entero positivo tal que a no es congruente ni con 0 ni con 1 módulo p y $a^q \equiv 1 \pmod{p}$.
- Probar que $q = \min\{n \in \mathbb{Z}^+ : a^n \equiv 1 \pmod{p}\}$.
 - Probar que $q|p-1$.
- c) Sea p primo y supongamos que existan 3 enteros a_1, a_2 y a_3 donde a_1 no es congruente ni con 0 ni con 1 módulo p y tal que $a_1^2 \equiv a_2 \pmod{p}, a_2^2 \equiv a_3 \pmod{p}$ y $a_3^2 \equiv a_1 \pmod{p}$.
- Probar que $p \equiv 1 \pmod{7}$.
 - Si se sabe que $361^2 \equiv 636 \pmod{p}, 636^2 \equiv 19 \pmod{p}$ y $19^2 \equiv 361 \pmod{p}$ donde p es un primo que verifica $700 \leq p \leq 725$, hallar p y calcular $361^{2^{361}} \pmod{p}$ (sugerencia: Método de exponenciación rápida).



Algunas identidades que pueden resultarles útiles para la parte 3b del ejercicio 2:

- $24623 \cdot 6803 - 26892 \cdot 6229 = 1$
- $30 \cdot 39 - 7 \cdot 167 = 1$
- $46 \cdot 39 - 11 \cdot 163 = 1$
- $128 \cdot 137 - 105 \cdot 167 = 1$
- $94 \cdot 137 - 79 \cdot 163 = 1$